Graduate Texts in Mathematics

Dinakar Ramakrishnan
Robert J. Valenza

Fourier Analysis on Number Fields

Springer

Graduate Texts in Mathematics 186

Springer Science+Business Media, LLC

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.

(continued after index)

Dinakar Ramakrishnan
Robert J. Valenza

Fourier Analysis on Number Fields

Springer

Dinakar Ramakrishnan
Mathematics Department
California Institute of Technology
Pasadena, CA 91125-0001
USA

Robert J. Valenza
Department of Mathematics
Claremont McKenna College
Claremont, CA 91711-5903
USA

Mathematics Subject Classification (1991): 42-01, 11F30

Library of Congress Cataloging-in-Publication Data
Ramakrishnan, Dinakar.
Fourier analysis on number fields / Dinakar Ramakrishnan, Robert J. Valenza.
p. cm. — (Graduate texts in mathematics ; 186)
Includes bibliographical references and index.
ISBN 978-1-4757-3087-6 ISBN 978-1-4757-3085-2 (eBook)
DOI 10.1007/978-1-4757-3085-2
1. Fourier analysis. 2. Topological groups. 3. Number theory.
I. Valenza, Robert J., 1951– . II. Title. III. Series
QA403.5.R327 1998
515′.2433—dc21 98-16715

Printed on acid-free paper.

Production managed by Terry Kornak; manufacturing supervised by Thomas King.
Photocomposed copy provided by the authors.

9 8 7 6 5 4 3 2 1

ISBN 978-1-4757-3087-6 SPIN 10659801

To Pat and Anand

To Brenda

Preface

This book grew out of notes from several courses that the first author has taught over the past nine years at the California Institute of Technology, and earlier at the Johns Hopkins University, Cornell University, the University of Chicago, and the University of Crete. Our general aim is to provide a modern approach to number theory through a blending of complementary algebraic and analytic perspectives, emphasizing harmonic analysis on topological groups. Our more particular goal is to cover John Tate's visionary thesis, giving virtually all of the necessary analytic details and topological preliminaries—technical prerequisites that are often foreign to the typical, more algebraically inclined number theorist. Most of the existing treatments of Tate's thesis, including Tate's own, range from terse to cryptic; our intent is to be more leisurely, more comprehensive, and more comprehensible. To this end we have assembled material that has admittedly been treated elsewhere, but not in a single volume with so much detail and not with our particular focus.

We address our text to students who have taken a year of graduate-level courses in algebra, analysis, and topology. While our choice of objects and methods is naturally guided by the specific mathematical goals of the text, our approach is by no means narrow. In fact, the subject matter at hand is germane not only to budding number theorists, but also to students of harmonic analysis or the representation theory of Lie groups. We hope, moreover, that our work will be a good reference for working mathematicians interested in any of these fields.

A brief sketch of each of the chapters follows.

(1) Topological Groups. The general discussion begins with basic notions and culminates with the proof of the existence and uniqueness of Haar (invariant) measures on locally compact groups. We next give a substantial introduction to profinite groups, which includes their characterization as compact, totally disconnected topological groups. The chapter concludes with the elementary theory of pro-p-groups, important examples of which surface later in connection with local fields.

(2) Some Representation Theory. In this chapter we introduce the fundamentals of representation theory for locally compact groups, with the ultimate

aim of proving certain key properties of unitary representations on Hilbert spaces. To reach this goal, we need some weighty analytic prerequisites, including an introduction to Gelfand theory for Banach algebras and the two spectral theorems. The first we prove completely; the second we only state, but with enough background to be thoroughly understandable. The material on Gelfand theory fortuitously appears again in the following chapter, in a somewhat different context.

(3) DUALITY FOR LOCALLY COMPACT ABELIAN GROUPS. The main points here are the abstract definition of the Fourier transform, the Fourier inversion formula, and the Pontryagin duality theorem. These require many preliminaries, including the analysis of functions of positive type, their relationship to unitary representations, and Bochner's theorem. A significant theme in all of this is the interplay between two alternative descriptions of the "natural" topology on the dual group of a locally compact abelian group. The more tractable description, as the compact-open topology, is presented in the first section; the other, which arises in connection with the Fourier transform, is introduced later as part of the proof of the Fourier inversion formula.

We have been greatly influenced here by the seminal paper on abstract harmonic analysis by H. Cartan and R. Godement (1947), although we give many more details than they, some of which are not obvious—even to experts. As a subsidiary goal of the book, we certainly hope that our exposition will encourage further circulation of their beautiful and powerful ideas.

(4) THE STRUCTURE OF ARITHMETIC FIELDS. In the first two sections the basics of local fields, such as the p-adic rationals $\mathbf{Q}_p$, are developed from a completely topological perspective; in this the influence of Weil's *Basic Number Theory* (1974) is apparent. We also provide some connections with the algebraic construction of these objects via discrete valuation rings. The remainder of the chapter deals with global fields, which encompass the finite extensions of $\mathbf{Q}$ and function fields in one variable over a finite field. We discuss places and completions, the notions of ramification index and residual degree, and some key points on local and global bases.

(5) ADELES, IDELES, AND THE CLASS GROUPS. This chapter establishes the fundamental topological properties of adele and idele groups and certain of their quotients. The first two sections lay the basic groundwork of definitions and elementary results. In the third, we prove the crucial theorem that a global field embeds as a cocompact subgroup of its adele group. We conclude, in the final section, with the introduction of the idele class group, a vast generalization of the ideal class group, and explain the relationship of the former to the more traditional ray class group.

(6) A QUICK TOUR OF CLASS FIELD THEORY. The material in this chapter is not logically prerequisite to the development of Tate's thesis, but it is used in our

subsequent applications. We begin with the Frobenius elements (conjugacy classes) associated with unramified primes P of a global field F, first in finite Galois extensions, next in the maximal extension unramified at P. In the next three sections we state the Tchebotarev density theorem, define the transfer map for groups, and state, without proof, the Artin reciprocity law for abelian extensions of global and local fields, in terms of the more modern language of idele classes. In the fifth and final section, we explicitly describe the cyclotomic extensions of $\mathbf{Q}$ and $\mathbf{Q}_p$ and then apply the reciprocity law to prove the Kronecker-Weber theorem for these two fields.

(7) TATE'S THESIS AND APPLICATIONS. Making use of the characters and duality of locally compact abelian groups arising from consideration of local and global fields, we carefully analyze the local and global zeta functions of Tate. This brings us to the main issue: the demonstration of the functional equation and analytic continuation of the L-functions of characters of the idele class group. There follows a proof of the regulator formula for number fields, which yields the residues of the zeta function of a number field F in terms of its class number h_F and the covolume of a lattice of the group U_F of units, in a suitable Euclidean space. From this we derive the class number formula and, in consequence, Dirichlet's theorem for quadratic number fields. Further investigation of these L-functions—in fact, some rather classical analysis—next yields another fundamental property: their nonvanishing on the line $\mathrm{Re}(s)=1$. Finally, as a most remarkable application of this material, we prove the following theorem of Hecke: Suppose that χ and χ' are idele class characters of a global field K and that $\chi_P=\chi_P'$ for a set of primes of positive density. Then $\chi=\mu\chi'$ for some character μ of finite order.

One of the more parenthetical highlights of this chapter (see Section 7.2) is the explanation of the analogy between the Poisson summation formula for number fields and the Riemann-Roch theorem for curves over finite fields.

We have given a number of exercises at the end of each chapter, together with hints, wherever we felt such were advisable. The difficult problems are often broken up into several smaller parts that are correspondingly more accessible. We hope that these will promote gradual progress and that the reader will take great satisfaction in ultimately deriving a striking result. We urge doing as many problems as possible; without this effort a deep understanding of the subject cannot be cultivated.

Perhaps of particular note is the substantial array of nonstandard exercises found at the end of Chapter 7. These span almost twenty pages, and over half of them provide nontrivial complements to, and applications of, the material developed in the chapter.

The material covered in this book leads directly into the following research areas.

- *L-functions of Galois Representations.* Following Artin, given a finite-dimensional, continuous complex representation σ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, one associates an L-function denoted $L(\sigma,s)$. Using Tate's thesis in combination with a theorem of Brauer and abelian class field theory, one can show that this function has a meromorphic continuation and functional equation. One of the major open problems of modern number theory is to obtain analogous results for l-adic Galois representations σ_l, where l is prime. This is known to be true for σ_l arising from abelian varieties of *CM* type, and $L(\sigma_l,s)$ is in this case a product of L-functions of idele class characters, as in Tate's thesis.

- *Jacquet-Langlands Theory.* For any reductive algebraic group G [for instance, $\mathrm{GL}_n(F)$ for a number field F], an important generalization of the set of idele class characters is given by the irreducible *automorphic* representations π of the locally compact group $G(\mathbf{A}_F)$. The associated *L-functions* $L(\pi,s)$ are well understood in a number of cases, for example for GL_n, and by an important conjecture of Langlands, the functions $L(\sigma_l,s)$ mentioned above are all expected to be expressible in terms of suitable $L(\pi,s)$. This is often described as nonabelian class field theory.

- *The p-adic L-functions.* In this volume we consider only complex-valued (smooth) functions on local and global groups. But if one fixes a prime p and replaces the target field $\mathbf{C}$ by $\mathbf{C}_p$, the completion of an algebraic closure of $\mathbf{Q}_p$, strikingly different phenomena result. Suitable p-adic measures lead to p-adic–valued L-functions, which seem to have many properties analogous to the classical complex-valued ones.

- *Adelic Strings.* Perhaps the most surprising application of Tate's thesis is to the study of string amplitudes in theoretical physics. This intriguing connection is not yet fully understood.

Acknowledgments

Finally, we wish to acknowledge the intellectual debt that this work owes to H. Cartan and R. Godement, J.-P. Serre (1968, 1989, and 1997), A. Weil, and, of course, to John Tate (1950). We also note the influence of other authors whose works were of particular value to the development of the analytic background in our first three chapters; most prominent among these are G. Folland (1984) and G. Pedersen (1989). (See References below for complete bibliographic data and other relevant sources.)

Contents

4 The Structure of Arithmetic Fields

5 Adeles, Ideles, and the Class Groups

6 A Quick Tour of Class Field Theory

7 Tate's Thesis and Applications

APPENDICES

Appendix A: Normed Linear Spaces

Appendix B: Dedekind Domains

Index of Notation

Notation	*Section*	*Interpretation*
$\mathbf{N}, \mathbf{Z}, \mathbf{Q}$	—	natural numbers, integers, and rational numbers, respectively
$\mathbf{R}, \mathbf{C}$	—	real and complex numbers, respectively
$\mathbf{R}_+, \mathbf{R}_+^\times$	—	nonnegative reals, positive reals
1_S	—	identity map on the set S
S^c	—	complement of the set S
$\mathrm{Card}(S)$	—	cardinality of the set S
$\bigsqcup S_\alpha$	—	disjoint union of sets S_α
$\mathrm{supp}(f)$	—	support of a function f
$\mathscr{C}(X)$	—	continuous (complex-valued) functions on a topological space X
$\mathscr{C}_c(X)$	—	continuous functions with compact support
$\mathscr{C}_c^+(X)$	—	positive elements of $\mathscr{C}_c(X)$ with positive sup norm
A^*, K^*	—	nonzero elements of a ring or field
$A^\times$	—	group of units of a ring A
$[K:F]$	—	degree of a finite field extension K/F
$N_{K/F}(x)$	—	norm map for a finite field extension K/F; see also Section 6.4
$\mathrm{tr}_{K/F}(x)$	—	trace map for a finite field extension K/F
KL	—	compositum of fields K and L
$\mathbf{Z}/n\mathbf{Z}$	—	integers modulo n
$\varphi(n)$	—	Euler phi function
S^1	—	the circle group
$W^\perp$	—	orthogonal complement of a subspace W
pr_W	—	orthogonal projection onto a subspace W

$k[[t]]$	—	ring of formal power series in t with coefficients in the field k
$k((t))$	—	fraction field of $k[[t]]$
$GL_n(k)$	—	group of invertible $n \times n$ matrices over k
$SL_n(k)$	—	$n \times n$ matrices over k of determinant 1
$B^1(X)$	A.1	unit ball in a normed linear space X
X^*	A.1	(norm) continuous dual of a normed linear space X
$l_1(\mathbf{C}^n)$	A.1	$\mathbf{C}^n$ with l_1 norm
$L(X)$	A.4	measurable functions on X modulo agreement almost everywhere
$L^p(X)$	A.4	L^p-space associated with a locally compact space X
$\Vert \cdot \Vert_p$	A.4	L^p-norm
A_S	B.1	localization of a ring A at subset S
J_K	B.2	set of fractional ideals of a global field K
P_K	B.2	set of principal fractional ideals of K
Cl_K	B.2	traditional class group of a global field K
$N(I)$	B.2	absolute norm map
$\Delta(x_1,\ldots,x_n)$	B.2	discriminant of a basis $x_1,\ldots,x_n$
$\Delta(B/A)$	B.2	discriminant ideal of a ring extension B/A
$L_h f$, $R_h f$	1.1	left and right translation operators on f
$(f:\varphi)$	1.2	Haar covering number
$\varprojlim G_i$	1.3	projective limit of a projective system $\{G_i\}$
$\hat{\mathbf{Z}}$	1.3	projective completion of $\mathbf{Z}$
$\mathbf{Z}_p$	1.3	ring of p-adic integers
G°	1.3	connected component of the identity
$\mathrm{Gal}(K/F)$	1.3	Galois group of the field extension K/F
F^S	1.3	fixed field of a set S of automorphisms of F
$\vert G \vert$	1.4	order of a profinite group G
$\mathrm{Aut}(V)$	2.1	algebraic automorphisms of a vector space
$\mathrm{Aut}_{\mathrm{top}}(V)$	2.1	topological automorphisms of a topological vector space
$\mathrm{Hom}(A,B)$	2.2	bounded operators between Banach spaces
$\mathrm{End}(A)$	2.2	endomorphisms on a Banach space A
$\Vert T \Vert$	2.2	norm of a bounded operator T

$\mathrm{sp}(a)$	2.2	spectrum of an element in a Banach algebra
$\mathrm{r}(a)$	2.2	spectral radius
$\hat{A}$	2.2	space of characters of a Banach algebra A
$\hat{a}$	2.2	Gelfand transform of a
$\mathscr{C}_0(X)$	2.3	continuous functions that vanish at infinity
T^*	2.3	adjoint of an operator T on a Hilbert space
$A_T \subseteq \mathrm{End}(H)$	2.3	the closed, self-adjoint, unital subalgebra generated by T in the ambient ring
$T^{1/2}$	2.3	square root of a positive operator
$\mathrm{Hom}_G(V, V')$	2.4	space of G-linear maps between two representation spaces
$\hat{G}$	3.1	Pontryagin dual of G
$X^{(n)} \subseteq G$	3.1	n-fold products within a group G
$W(K,V)$	3.1	local basis sets for the compact-open topology
$N(\varepsilon) \subseteq S^1$	3.1	ε-neighborhood of the identity in S^1
V_φ	3.2	Hilbert space associated with φ
$f*g$	3.2	convolution of functions
$\mathscr{P}(G)$	3.2	continuous function of positive type, bounded by 1 on G
$\mathscr{E}(G)$	3.2	elementary functions on G
$\hat{f}$	3.3	Fourier transform of a function f
$V(G)$	3.3	complex span of continuous functions of positive type
$V^1(G)$	3.3	L^1-functions in $V(G)$
$T_{\hat{\mu}}$	3.3	Fourier transform of a measure $\hat{\mu}$
$\mathrm{mod}_G(\alpha)$	4.1	module of an automorphism α on G
$B_m \subseteq k$	4.1	ball of module radius m in a topological field k
$\mathrm{ord}_k(a)$	4.2	order of an element of a local field k
$\lvert\cdot\rvert_p, \lvert\cdot\rvert_\infty$	4.2	p-norm and infinity norm on $\mathbf{Q}$ or $\mathbf{F}_q(t)$; see also Section 4.3
$\pi = \pi_k$	4.2	uniformizing parameter for a local field k
$e = e(k_1/k)$	4.3	ramification index of an extension of local fields

$f=f(k_1/k)$	4.3	residual degree of an extension of local fields
K_v	4.4	completion of a field K at a place v
K_Q	4.4	completion of global field K at the place corresponding to a prime Q
$\mathscr{P}_K$	4.4	set of places of K
$\mathscr{P}_{K,\infty}$	4.4	set of Archimedean places of K
$\mathscr{P}_{K,f}$	4.4	set of ultrametric places of K
$r_{K/F}: \mathscr{P}_K \to \mathscr{P}_F$	4.4	restriction map for places of a field extension K/F
$v\|u$	4.4	place v restricts to place u
$\mathfrak{o}_v$	4.4	local ring of integers with respect to a place v
$\mathfrak{o}_K$	4.4	ring of integers of a global field K
D_Q	4.5	decomposition group of a prime Q
ρ_Q	4.5	canonical map from D_Q to $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F})$
j_Q	4.5	induced isomorphism from D_Q onto $\mathrm{Gal}(K_Q/F_P)$ where Q lies over P
$\mathrm{Hom}_k(L,M)$	4.5	embedding of L into M over k
$\Pi' G_v$	5.1	restricted direct product
G_S	5.1	S-version of the restricted direct product
$\prod_v dg_v$	5.1	induced Haar measure on a restricted direct product of locally compact groups
$\mathbf{A}_K$	5.2	adele group of a global field K
$\mathbf{I}_K$	5.2	idele group of a global field K
S_ω	5.2	set of infinite places of a global field
$\mathbf{A}_\omega$	5.2	the open subgroup $\mathbf{A}_{S_\omega}$ of the adele group
C_K	5.4	idele class group of global field K; see also Section 6.4
$\|x\|_{\mathbf{A}_K}$	5.4	standard absolute value on the adele group
$C_K^1 = \mathbf{I}_K^1/K^*$	5.4	norm-one idele class group
S_∞	5.4	set of Archimedean places of a global field
$\mathbf{I}_{K,S}$	5.4	S-ideles of the global field K
$\mathbf{I}_{K,S}^1$	5.4	S-ideles of norm one
R_S	5.4	S-integers of a global field
$\mathbf{A}_{K,S}$	5.4	S-adeles of the global field K

$C_{K,S}$	5.4	S-class group of a global field K
v_P	5.4	discrete valuation associated with a prime P in a Dedekind domain
$K_{M,1}$	5.4	elements of K congruent to 1 modulo the integral ideal M
$J_K(M)$	5.4	fractional ideals relatively prime to M
$Cl_K(M)$	5.4	wide ray class group of K relative to M
$K_{\widetilde{M},1}$	5.4	elements of K congruent to 1 modulo the ideal M extended by a set of real places
$Cl_K(\widetilde{M})$	5.4	narrow ray class group of K relative to $\widetilde{M}$
$\varphi_{Q/P}$	6.1	Frobenius element associated with primes Q and P, where Q lies over P
$(P,K/F)$	6.1	Artin symbol (or Frobenius class)
$F^{\mathrm{ur}}(P)$	6.1	maximal unramified extension of F at P
Σ_F	6.2	set of places of a global field F
(G,G)	6.3	commutator subgroup of a group G
G^{ab}	6.3	abelianization of a group G
$V: G^{\mathrm{ab}} \to H^{\mathrm{ab}}$	6.3	transfer map
C_F	6.4	idele class group for F global, F^* for F local
$N_{K/F}: C_K \to C_F$	6.4	norm homomorphism
$j_{K/F}: C_F \to C_K$	6.4	map induced by inclusion
$\Gamma_K = \mathrm{Gal}\ \overline{F}/K)$	6.4	Galois group of the separable closure of F over a finite extension K of F
$i_{K/F}: \Gamma_K \to \Gamma_F$	6.4	inclusion map of Galois groups
$V: \Gamma_F^{\mathrm{ab}} \to \Gamma_K^{\mathrm{ab}}$	6.4	transfer map on Galois groups
$\theta_F: C_F \to \Gamma_F^{\mathrm{ab}}$	6.4	Artin map
$\theta_{K/F}$	6.4	Artin map with projection onto $\mathrm{Gal}(K/F)$
F^{ab}	6.5	maximal abelian extension of a field F
F_n	6.5	extension of F by all nth roots of unity
F_∞	6.5	extension of F by *all* roots of unity
$\theta(z)$	7.0	theta function
$d^*x = dx/\lvert x\rvert$	7.1	Haar measure on F^* as given by the Haar measure dx on a local field F
U_F	7.1	elements of F^* of unit absolute value
$\mathcal{G}_F$	7.1	valuation group of a local field F

$X(F^*)$	7.1	characters of a local field F
$L(\chi)$ or $L(s,\chi)$	7.1	local L-factor associated with a local character χ; see also Section 7.4
$\Gamma(s)$	7.1	ordinary gamma function
$\Gamma_F(s)$	7.1	gamma function associated with $F=\mathbf{R}$ or $\mathbf{C}$
$\mathrm{sgn}(x)$	7.1	sign character
$\chi^\vee = \chi^{-1}\lvert\cdot\rvert$	7.1	shifted dual of a character χ
ψ_a	7.1	multiplicative translate of an additive character by a field element a
$S(F)$	7.1	space of Schwartz-Bruhat functions on F
$Z(f,\chi)$	7.1	local zeta function; see also Section 7.3
$\mathfrak{o}'_F$	7.1	dual of $\mathfrak{o}_F$ with respect to the trace map
$\mathcal{D}_F$	7.1	different of a field F
ψ_F	7.1	standard character of a local field F
$g(\omega,\lambda)$	7.1	Gauss sum for characters ω and λ
$W(\omega)$	7.1	root number associated with a character ω
$S(\mathbf{A}_K)$	7.2	adelic Schwartz-Bruhat functions
$\tilde{\varphi}(x)$	7.2	average value of $\varphi\in S(\mathbf{A}_K)$ over K
$\mathrm{Div}(K)$	7.2	divisor group of a function field K
$\mathrm{Div}^0(K)$	7.2	group of divisors of degree zero
$\deg(D)$	7.2	degree of a divisor D
$\mathrm{div}(f)$	7.2	principal divisor associated with f
$\mathrm{div}(x)$	7.2	divisor function extended to ideles; see also Section 7.5
$\mathrm{Pic}(K)$	7.2	Picard group of a function field K
$\mathrm{Pic}^0(K)$	7.2	Picard group of degree zero
$L(D)$	7.2	linear system associated with a divisor D
$l(D)$	7.2	dimension of the vector space $L(D)$
ψ_K	7.3	standard character of a global field K
$\mathcal{D}_P$	7.3	local different at P of a global field
$Z(f,\chi)$	7.3	global zeta function
$L(s,\chi)$	7.4	Hecke L-function associated with a global character χ
$L(s,\chi_f)$	7.4	finite version of $L(s,\chi)$
$L(s,\chi_\infty)$	7.4	infinite version of $L(s,\chi)$
$\zeta(s)$	7.4	Riemann zeta function

1
Topological Groups

Our work begins with the development of a topological framework for the key elements of our subject. The first section introduces the category of topological groups and their fundamental properties. We treat, in particular, uniform continuity, separation properties, and quotient spaces. In the second section we narrow our focus to locally compact groups, which serve as the locale for the most important mathematical phenomena treated subsequently. We establish the essential deep feature of such groups: the existence and uniqueness of Haar measure; this is fundamental to the development of abstract harmonic analysis. The last two sections further specialize to profinite groups, giving a topological characterization, a structure theorem, and a set of results roughly analogous to the Sylow Theorems for finite groups. The prerequisites for this discussion will be found in almost any first-year graduate courses in algebra and analysis.

1.1 Basic Notions

DEFINITION. A *topological group* is a group G (identity denoted e) together with a topology such that the following conditions hold:

(i) The group operation

$$\begin{aligned} G \times G &\to G \\ (g,h) &\mapsto gh \end{aligned}$$

is a continuous mapping. (The domain has the product topology.)

(ii) The inversion map

$$\begin{aligned} G &\to G \\ g &\mapsto g^{-1} \end{aligned}$$

is likewise continuous.

By convention, whenever we speak of a finite topological group, we intend the discrete topology.

Clearly the class of topological groups together with continuous homomorphisms constitutes a category.

It follows at once that translation (on either side) by any given group element is a homeomorphism $G \to G$. Thus the topology is *translation invariant* in the sense that for all $g \in G$ and $U \subseteq G$ the following three assertions are equivalent:

(i) U is open.

(ii) gU is open.

(iii) Ug is open.

Moreover, since inversion is likewise a homeomorphism, U is open if and only if $U^{-1} = \{x : x^{-1} \in U\}$ is open.

A fundamental aspect of a topological group is its *homogeneity*. In general, if X is any topological space, Homeo(X) denotes the set of all homeomorphisms $X \to X$. If S is a subset of Homeo(X), then one says that X is a *homogeneous space under* S if for all $x,y \in X$, there exists $f \in S$ such that $f(x)=y$. (When S is unspecified or perhaps all of Homeo(X), one says simply that X is a *homogeneous space.*) Clearly any topological group G is homogeneous under itself in the sense that given any points $g,h \in G$, the homeomorphism defined as left translation by hg^{-1} (i.e., $x \mapsto hg^{-1}x$) sends g to h. From this it follows at once that a local base at the identity $e \in G$ determines a local base at any point in G, and in consequence the entire topology.

EXAMPLES

(1) Any group G is a topological group with respect to the discrete topology.

(2) $\mathbf{R}^*$, $\mathbf{R}^*_+$, and $\mathbf{C}^*$ are topological groups with respect to ordinary multiplication and the Euclidean topology.

(3) $\mathbf{R}^n$ and $\mathbf{C}^n$ are topological groups with respect to vector addition and the Euclidean topology.

(4) Let $k = \mathbf{R}$ or $\mathbf{C}$. Then the general linear group

$$\mathrm{GL}_n(k) = \{g \in M_n(k) : \det(g) \neq 0\} \quad (n \geq 1)$$

is a topological group with respect to matrix multiplication and the Euclidean topology. The special linear group

$$\mathrm{SL}_n(k) = \{g \in \mathrm{GL}_n(k) : \det(g) = 1\} \quad (n \geq 1)$$

is a closed subgroup of $\mathrm{GL}_n(k)$.

In subsequent discussion, if X is a topological space and $x \in X$, we shall say that $U \subseteq X$ is a *neighborhood of* x if x lies in the interior of U (i.e., the largest open subset contained in U). Thus a neighborhood need not be open, and it makes sense to speak of a closed or compact neighborhood, as the case may be.

A subset S of G is called *symmetric* if $S=S^{-1}$. This is a purely group-theoretic concept that occurs in the following technical proposition.

1-1 PROPOSITION. *Let G be a topological group. Then the following assertions hold:*

(i) *Every neighborhood U of the identity contains a neighborhood V of the identity such that $VV \subseteq U$.*

(ii) *Every neighborhood U of the identity contains a symmetric neighborhood V of the identity.*

(iii) *If H is a subgroup of G, so is its closure.*

(iv) *Every open subgroup of G is also closed.*

(v) *If K_1 and K_2 are compact subsets of G, so is K_1K_2.*

PROOF. (i) Certainly we may assume that U is open. Consider the continuous map $\varphi: U \times U \to G$ defined by the group operation. Certainly $\varphi^{-1}(U)$ is open and contains the point (e,e). By definition of the topology on $U \times U$, there exist open subsets V_1, V_2 of U such that $(e,e) \in V_1 \times V_2$. Set $V=V_1 \cap V_2$. Then V is a neighborhood of e contained in U such that by construction $VV \subseteq U$.

(ii) Clearly $g \in U \cap U^{-1} \Leftrightarrow g, g^{-1} \in U$, so $V = U \cap U^{-1}$ is the required symmetric neighborhood of e.

(iii) Any two points g and h in the closure of H may be exhibited as the limits of convergent nets in H itself. Hence by continuity their product is likewise the limit of a convergent net in H and similarly for inverses.

(iv) If H is any subgroup of G, then G is the disjoint union of the cosets of H, and hence H itself is the complement of the union of its nontrivial translates. If H is open, so are these translates, whence H is the complement of an open set and therefore closed.

(v) K_1K_2 is the image of the compact set $K_1 \times K_2$ under the continuous map $(k_1, k_2) \mapsto k_1k_2$. It is therefore compact by general topology ❑

Note that (i) and (ii) together imply that every neighborhood U of the identity contains a symmetric neighborhood V such that $VV \subseteq U$.

Translation of Functions and Uniform Continuity

Given an arbitrary function f on a group, we define its *left* and *right translates* by the formulas

$$L_hf(g)=f(h^{-1}g) \quad \text{and} \quad R_hf(g)=f(gh) \ .$$

If f is a (real- or complex-valued) continuous function on a topological group, we say that f is *left uniformly continuous* if for every $\varepsilon>0$ there is a neighborhood V of e such that

$$h \in V \Rightarrow \| L_hf - f \|_u < \varepsilon$$

where $\| \ \|_u$ denotes the uniform, or sup, norm. Right uniform continuity is defined similarly. Recall that $\mathscr{C}_c(G)$ denotes the set of continuous functions on G with compact support.

1-2 PROPOSITION. *Let G be a topological group. Then every function f in $\mathscr{C}_c(G)$ is both left and right uniformly continuous.*

PROOF. We prove right uniform continuity. Let $K=\text{supp}(f)$ and fix $\varepsilon>0$. Then for every $g\in K$ there exists an open neighborhood U_g of the identity such that

$$h \in U_g \Rightarrow |f(gh)-f(g)|<\varepsilon \ .$$

Equivalently, $f(g')$ is ε-close to $f(g)$ whenever $g^{-1}g'$ lies in U_g. Moreover, by the comment following the previous proposition, each U_g contains an open symmetric neighborhood V_g of the identity such that $V_gV_g\subseteq U_g$. Clearly the collection of subsets gV_g covers K, and a finite subcollection $\{g_jV_j\}_{j=1,\dots,n}$ suffices. Henceforth we write V_j for V_{g_j} and U_j for U_{g_j}. Define V, a symmetric open neighborhood of the identity e, by the formula

$$V=\bigcap_{j=1}^{n} V_j \ .$$

If $g\in K$, then $g\in g_jV_j$ for some j. For $h\in V$ we consider the difference $f(gh)-f(g)$:

$$|f(gh)-f(g)| \le |f(gh)-f(g_j)| + |f(g_j)-f(g)| \ .$$

The point is that both $g_j^{-1}g$ and $g_j^{-1}gh$ lie in U_j, so that both terms on the right are bounded by ε. (Here is where we use that property $V_jV_j\subseteq U_j$ for all j.) This establishes right uniform continuity for K.

When g does not lie in K, then we must bound $|f(gh)|$. If $f(gh)\neq 0$, then $gh\in g_jV_j$ for some j, and therefore $f(gh)$ is ε-close to $f(g_j)$. Moreover, $g_j^{-1}g=g_j^{-1}ghh^{-1}$ lies in U_j (here is where we use the symmetry of V), and it follows that $|f(g_j)|<\varepsilon$ since g_j is close to g and $f(g)=0$ by assumption. Consequently $|f(gh)|<2\varepsilon$, and the argument is complete. ❑

Separation Properties and Quotient Spaces

Some authors assume as part of the definition of a topological group that the underlying topology is T_1. In this case it is also customary to reserve the term *subgroup* for a closed subset that constitutes a subgroup in the ordinary algebraic sense. Note that in general we accept neither of these assumptions.

The following proposition shows, among other things, that for a topological group the separation axioms T_1 and T_2 (Hausdorff) have equal strength.

1-3 PROPOSITION. *Let G be a topological group. Then the following assertions are equivalent:*

(i) *G is T_1.*

(ii) *G is Hausdorff.*

(iii) *The identity e is closed in G.*

(iv) *Every point of G is closed.*

PROOF. (i)$\Rightarrow$(ii) If G is T_1, then for any distinct $g,h\in G$ there is an open neighborhood U of the identity lacking gh^{-1}. According to Proposition 1-1, U admits a symmetric open subset V, also containing the identity, such that $VV\subseteq U$. Then Vg and Vh are disjoint open neighborhoods of g and h, since otherwise gh^{-1} lies in $V^{-1}V=VV\subseteq U$.

(ii)$\Rightarrow$(iii) Every point in a Hausdorff (or merely T_1) space is closed.

(iii)$\Rightarrow$(iv) This is a consequence of homogeneity: For every point $x\in G$ there is a homeomorphism that carries e onto x. Hence if e is closed, so is every point.

(iv)$\Rightarrow$(i) Obvious by general topology. ❑

If H is a subgroup of the topological group G, then the set G/H of left cosets of G acquires the *quotient topology*, defined as the strongest topology such that the canonical projection $\rho{:}\,g\mapsto gH$ is continuous. Thus U is open in G/H if and only if $\rho^{-1}(U)$ is open in G. Recall from algebra that G/H constitutes a group under coset multiplication if and only if H is moreover normal in G. We shall see shortly that in this case G/H also constitutes a topological group with respect to the quotient topology.

The following two propositions summarize some of the most important properties of the quotient construction.

1-4 PROPOSITION. *Let G be a topological group and let H be a subgroup of G. Then the following assertions hold:*

(i) *The quotient space G/H is homogeneous under G.*

(ii) *The canonical projection $\rho: G \to G/H$ is an open map.*

(iii) *The quotient space G/H is T_1 if and only if H is closed.*

(iv) *The quotient space G/H is discrete if and only if H is open. Moreover, if G is compact, then H is open if and only if G/H is finite.*

(v) *If H is normal in G, then G/H is a topological group with respect to the quotient operation and the quotient topology.*

(vi) *Let H be the closure of $\{e\}$ in G. Then H is normal in G, and the quotient group G/H is Hausdorff with respect to the quotient topology.*

PROOF. (i) An element $x \in G$ acts on G/H by left translation: $gH \mapsto xgH$. The inverse map takes the same form, so to show that left translation is a homeomorphism of G/H, it suffices to show that left translation is an open mapping on the quotient space. Let $\overline{U}$ be an open subset of G/H. By definition of the quotient topology, the inverse image of $\overline{U}$ under ρ is an open subset U of G, and it follows that the inverse image of $g\overline{U}$ under ρ is gU, also an open subset of G. Therefore $g\overline{U}$ is open, and left translation is indeed an open map, as required.

(ii) Let V be an open subset of G. We must show that $\rho(V)$ is open in the quotient. But $\rho(V)$ is open in G/H if and only if $\rho^{-1}(\rho(V))$ is open in G. By elementary group theory, $\rho^{-1}(\rho(V)) = V \cdot H$. Let x lie in $V \cdot H$, so that $x = vh$ for some $v \in V$ and $h \in H$. Since V is open, given any $v \in V$, there is an open neighborhood $U_v \subseteq V$ containing v. Thus $U_v \cdot h$ is an open neighborhood of x contained in $V \cdot H$, which is accordingly open.

(iii) By general topology, G/H is T_1 if and only if every point is closed. Since a coset of H is its own inverse image under projection, each coset is a closed point in G/H if and only if each is likewise a closed subset of G. But by homogeneity this is the case if and only if H itself is closed in G. (Note that we cannot appeal to the previous proposition, since the topological space G/H is not necessarily a topological group with respect to multiplication of cosets.)

(iv) Let H be a subgroup of G. Then by part (ii), H is an open subset of G if and only if H is an open point of G/H. Since G/H is homogeneous under G, this

holds if and only if G/H is discrete. Assume now that G is compact. Then so is G/H, since ρ is continuous. But then H is open if and only if G/H is both compact and discrete, which is to say, if and only if G/H is finite. (Recall our convention that a finite topological group carries the discrete topology.)

(v) Assume that H is a normal subgroup of G. Then from part (ii) and the commutative diagram

$$\begin{array}{ccc} G & \xrightarrow{T_g} & G \\ \rho\downarrow & & \downarrow\rho \\ G/H & \xrightarrow{T_{\rho(g)}} & G/H \end{array}$$

(where T_g denotes left translation by g), we see at once that translation by any group element is continuous on the quotient. A similar diagram establishes the continuity of the inversion map.

(vi) Since $\{e\}$ is a subgroup of G, so is its closure H. Moreover, it is the smallest closed subgroup of G containing e and therefore normal, since each conjugate of H is likewise a closed subgroup containing e. In light of the previous proposition, the full assertion now follows from parts (iii) and (v) above. ❑

Part (vi) shows that every topological group projects by a continuous homomorphism onto a topological group with Hausdorff topology. In this sense the assumption that a given group is Hausdorff is not too serious.

1-5 PROPOSITION. *Let G be a Hausdorff topological group. Then the following assertions hold:*

(i) *The product of a closed subset F and a compact subset K is closed.*

(ii) *If H is a compact subgroup of G, then $\rho: G \to G/H$ is a closed map.*

PROOF. (i) Let z lie in the closure of the product FK. Then there exists a net converging to z of the form $\{x_\alpha y_\alpha\}$ with $x_\alpha \in F$ and $y_\alpha \in K$. Since K is compact, we may replace our given net by a subnet such that $\{y_\alpha\}$ converges to some point y in K. We claim that this forces the convergence of $\{x_\alpha\}$ in F to zy^{-1}, showing that $z = zy^{-1}y$ lies in FK, which is therefore closed. To establish the claim, consider an arbitrary open neighborhood U of the identity e. We may choose yet another neighborhood of e contained in U such that $VV \subseteq U$. Then the nets $\{z^{-1}x_\alpha y_\alpha\}$ and $\{y_\alpha^{-1}y\}$ are both eventually in V, whence the product $z^{-1}x_\alpha y_\alpha y_\alpha^{-1} y = z^{-1}x_\alpha y$ is eventually in U. Thus $\lim x_\alpha = zy^{-1}$, as required.

(ii) If X is a closed subset of G, then arguing as the second part of the previous proposition, we are reduced to showing that $X{\cdot}H$ is likewise a closed subset of G. But if H is compact, this is just a special case of assertion (i). ❑

REMARK. The requirement that H be compact is essential. For example, in the case $G=\mathbf{R}^2$, with subgroup $H=\{(0,y):y\in\mathbf{R}\}$, we have clearly $G/H\cong\mathbf{R}$, and under this identification, $\rho(x,y)=x$. Now let $X=\{(x,y)\in\mathbf{R}^2 : xy=1\}$. Then X is closed, but $\rho(X)=\mathbf{R}^*$ is not.

Locally Compact Groups

Recall that a topological space is called *locally compact* if every point admits a compact neighborhood.

DEFINITION. A topological group G that is both locally compact and Hausdorff is called a *locally compact group.*

Note well the assumption that a locally compact group is Hausdorff. Accordingly, all points are closed.

1-6 PROPOSITION. *Let G be a Hausdorff topological group. Then a subgroup H of G that is locally compact (in the subspace topology) is moreover closed. In particular, every discrete subgroup of G is closed.*

PROOF. Let K be a compact neighborhood of e in H. Then K is closed in H, since H is likewise Hausdorff, and therefore there exists a closed neighborhood U of e in G such that $K=U\cap H$. Since $U\cap H$ is compact in H, it is also compact in G, and therefore also closed. By Proposition 1-1, part (i), there exists a neighborhood V of e in G such that $VV\subseteq U$. We shall now show that $x\in\overline{H}\Rightarrow x\in H$.

First note that $\overline{H}$ is a subgroup of G by Proposition 1-1, part (iii). Thus if $x\in\overline{H}$, then every neighborhood of x^{-1} meets H. In particular, there exists some $y\in Vx^{-1}\cap H$. We claim that the product yx lies in $U\cap H$. Granting this, both y and yx lie in the subgroup H, whence so does x, as required.

PROOF OF CLAIM. Since $U\cap H$ is closed, it suffices to show that every neighborhood W of yx meets $U\cap H$. Since $y^{-1}W$ is a neighborhood of x, so is $y^{-1}W\cap xV$. Moreover, by assumption x lies in the closure of H, so there exists some element $z\in y^{-1}W\cap xV\cap H$. Now consider:

(i) the product yz lies both in W and in the subgroup H;

(ii) by construction, $y\in Vx^{-1}$;

(iii) by construction, $z\in xV$.

The upshot is that yz lies in $Vx^{-1}\cdot xV=VV$, a subset of U, and therefore the intersection $W\cap(U\cap H)$ is nonempty. This establishes the claim and thus completes the proof. ❑

1.2 Haar Measure

We first recall a sequence of fundamental definitions from analysis that culminate in the definition of a Haar measure. We shall then establish both its existence and uniqueness for locally compact groups.

A collection $\mathfrak{M}$ of subsets of a set X is called a *σ-algebra* if it satisfies the following conditions:

(i) $X\in\mathfrak{M}$.

(ii) If $A\in\mathfrak{M}$, then $A^c\in\mathfrak{M}$, where A^c denotes the complement of A in X.

(iii) Suppose that $A_n\in\mathfrak{M}$ $(n\geq 1)$, and let

$$A=\bigcup_{n=1}^{\infty}A_n \quad .$$

Then also $A\in\mathfrak{M}$; that is, $\mathfrak{M}$ is closed under countable unions.

It follows from these axioms that the empty set is in $\mathfrak{M}$ and that $\mathfrak{M}$ is closed under finite and countably infinite intersections.

A set X together with a σ-algebra of subsets $\mathfrak{M}$ is called a *measurable space*. If X is moreover a topological space, we may consider the smallest σ-algebra $\mathscr{B}$ containing all of the open sets of X. The elements of $\mathscr{B}$ are called the *Borel subsets* of X.

A *positive measure* μ on an arbitrary measurable space $\langle X,\mathfrak{M}\rangle$ is a function $\mu:\mathfrak{M}\rightarrow\mathbf{R}_+\cup\{\infty\}$ that is *countably additive*; that is,

$$\mu\left(\bigcup_{n=1}^{\infty}A_n\right)=\sum_{n=1}^{\infty}\mu(A_n)$$

for any family $\{A_n\}$ of disjoint sets in $\mathfrak{M}$. In particular, a positive measure defined on the Borel sets of a locally compact Hausdorff space X is called a *Borel measure*.

Let μ be a Borel measure on a locally compact Hausdorff space X, and let E be a Borel subset of X. We say that μ is *outer regular* on E if

$$\mu(E)=\inf\{\mu(U):U\supseteq E,\ U\text{ open}\} \quad .$$

We say that μ is *inner regular* on E if

$$\mu(E) = \sup\{\mu(K) : K \subseteq E, K \text{ compact}\} \ .$$

A *Radon measure* on X is a Borel measure that is finite on compact sets, outer regular on all Borel sets, and inner regular on all open sets. One can show that a Radon measure is, moreover, inner regular on σ-finite sets (that is, countable unions of μ-measurable sets of finite measure).

Let G be a group and let μ be a Borel measure on G. We say that μ is *left translation invariant* if for all Borel subsets E of G,

$$\mu(sE) = \mu(E)$$

for all $s \in G$. *Right translation invariance* is defined similarly.

DEFINITION. Let G be a locally compact topological group. Then a *left* (respectively, *right*) *Haar measure* on G is a nonzero Radon measure μ on G that is left (respectively, right) translation-invariant. A *bi-invariant Haar measure* is a nonzero Radon measure that is both left and right invariant.

The following proposition shows that the existence of a left Haar measure is equivalent to the existence of a right Haar measure and, in a sense, equates the translation invariance of measure with that of integration. As usual, we let

$$\mathscr{C}_c^+(G) = \{f \in \mathscr{C}_c(G) : f(s) \geq 0 \ \forall s \in G \text{ and } \|f\|_u > 0\} \ .$$

We often abbreviate this to $\mathscr{C}_c^+$ when the domain is clear.

1-7 PROPOSITION. *Let G be a locally compact group with nonzero Radon measure μ. Then:*

(i) *The measure μ is a left Haar measure on G if and only if the measure $\tilde{\mu}$ defined by $\tilde{\mu}(E) = \mu(E^{-1})$ is a right Haar measure on G.*

(ii) *The measure μ is a left Haar measure on G if and only if*

$$\int_G L_s f \, d\mu = \int_G f \, d\mu$$

for all $f \in \mathscr{C}_c^+$ and $s \in G$.

(iii) *If μ is a left Haar measure on G, then μ is positive on all nonempty open subsets of G and*

$$\int_G f\,d\mu > 0$$

for all $f \in \mathscr{C}_c^+$.

(iv) *If* μ *is a left Haar measure on G, then* $\mu(G)$ *is finite if and only if G is compact.*

PROOF. (i) By definition, we have the equivalence

$$\tilde{\mu}(E) = \tilde{\mu}(Es)\ \forall s \in G \iff \mu(E^{-1}) = \mu(s^{-1}E^{-1})\ \forall s \in G$$

for all Borel sets E; the assertion follows at once. (For *any* topological group G, clearly E is a Borel subset of G if and only if E^{-1} is.)

(ii) If μ is a Haar measure on G, then the stated equality of integrals follows by definition for all simple functions $f \in \mathscr{C}_c^+$ (i.e., finite linear combinations of characteristic functions on G), and hence, by taking limits, for arbitrary $f \in \mathscr{C}_c^+$. Conversely, from the positive linear functional $\int_G \cdot\, d\mu$ on $\mathscr{C}_c(G)$ we can, by the Riesz representation theorem, explicitly recover the Radon measure μ of any open subset $U \subseteq G$ as follows:

$$\mu(U) = \sup\{\int_G f\,d\mu : f \in \mathscr{C}_c(G),\ \|f\|_u \le 1, \text{ and } \operatorname{supp}(f) \subseteq U\}\ .$$

From this one sees at once that if the integral is left translation invariant, then $\mu(sU) = \mu(U)$ for all open subsets U of G, since $\operatorname{supp}(f) \subseteq U$ if and only if $\operatorname{supp}(L_s f) \subseteq sU$. The result now extends to all Borel subsets of G because a Radon measure is by definition outer regular.

(iii) Since μ is not identically 0, by inner regularity there is a compact set K such that $\mu(K)$ is positive. Let U be any nonempty open subset of G. Then from the inclusion

$$K \subseteq \bigcup_{s \in G} sU$$

we deduce that K is covered by a finite set of translates of U, all of which must have equal measure. Thus since $\mu(K)$ is positive, so is $\mu(U)$. If $f \in \mathscr{C}_c^+$, then there exists a nonempty open subset U of G on which f exceeds some positive constant R. It then follows that

$$\int_G f\,d\mu \ge R\mu(U) > 0$$

as claimed.

(iv) If G is compact, then certainly $\mu(G)$ is finite by definition of a Radon measure. To establish the converse, assume that G is not compact. Let K be a compact set whose interior contains e. Then no finite set of translates of K covers G (which would otherwise be compact), and there must exist an infinite sequence $\{s_j\}$ in G such that

$$s_n \notin \bigcup_{j<n} s_j K \quad . \tag{1.1}$$

Now K contains a symmetric neighborhood U of e such that $UU \subseteq K$. We claim that the translates $s_j U$ $(j \geq 1)$ are disjoint, from which it follows at once from (iii) that $\mu(G)$ is infinite.

PROOF OF CLAIM. Suppose that for $i<j$ we have $s_i u = s_j v$ where $u,v \in U$. Then $s_j = s_i uv^{-1} \in s_i K$, since U is symmetric and $UU \subseteq K$. But this contradicts Eq. 1.1. ❑

With these preliminaries completed, we now come to one of the major theorems in analysis.

1-8 THEOREM. *Let G be a locally compact group. Then G admits a left (hence right) Haar measure. Moreover, this measure is unique up to a scalar multiple.*

Via the Riesz representation theorem and statement (ii) of the previous proposition, the existence part of the proof reduces to the construction of a left-invariant linear functional on $\mathscr{C}_c(G)$. The key idea is the introduction of a translation-invariant device for comparing functions in $\mathscr{C}_c^+$.

Preliminaries to the Existence Proof

Let $f, \varphi \in \mathscr{C}_c^+$. Set $U=\{s \in G : \varphi(s) > \|\varphi\|_u/2\}$, so that a finite number of translates of the open set U suffice to cover supp(f). Then there are n elements $s_1, \ldots, s_n \in G$ such that a linear combination of the translates of φ by the s_j dominates f in the following sense:

$$f \leq \frac{2\|f\|_u}{\|\varphi\|_u} \sum_{j=1}^{n} L_{s_j} \varphi \quad .$$

The point is that if $s \in \text{supp}(f)$, then $s \in s_j U$ for some j, so that $s_j^{-1} s \in U$ if φ is sufficiently large. Thus it makes sense to define $(f:g)$, *the Haar covering number* of f with respect to φ, by the formula

$$(f:\varphi) = \inf\left\{\sum_{j=1}^{n} c_j : 0 < c_1,\ldots,c_n \text{ and } f \leq \sum_{j=1}^{n} c_j L_{s_j}\varphi \text{ for some } s_1,\ldots,s_n \in G\right\}.$$

Note that since $\|f\|_u$ is assumed positive, the Haar covering number is never zero. We shall see shortly that $(f:\varphi)$ is almost linear in f for appropriately chosen φ.

1-9 LEMMA. *The Haar covering number has the following properties:*

(i) $(f:\varphi) = (L_s f:\varphi)$ *for all* $s\in G$

(ii) $(f_1+f_2:\varphi) \leq (f_1:\varphi) + (f_2:\varphi)$

(iii) $(cf:\varphi) = c(f:\varphi)$ *for any* $c>0$

(iv) $(f_1:\varphi) \leq (f_2:\varphi)$ *whenever* $f_1 \leq f_2$

(v) $(f:\varphi) \geq \|f\|_u/\|\varphi\|_u$

(vi) $(f_1:\varphi) \leq (f_1:f_0)(f_0:\varphi)$

PROOF. (i) Since left multiplication by any given group element constitutes a permutation of the ambient group, for all $s\in G$ we have the equivalence

$$f(t) \leq \sum c_j L_{s_j}\varphi(t)\ \forall t \in G \Leftrightarrow L_s f(t) \leq \sum c_j L_{ss_j}\varphi(t)\ \forall t \in G$$

which is to say that

$$f \leq \sum c_j L_{s_j}\varphi \Leftrightarrow L_s f \leq \sum c_j L_{ss_j}\varphi \ .$$

Hence precisely the same sets of coefficients c_j occur in the calculation of $(f:\varphi)$ as for $(L_s f:\varphi)$.

(ii), (iii), (iv) Obvious.

(v) If the coefficients c_j appear in the calculation of $(f:\varphi)$, then

$$f(s) \leq \sum c_j\varphi(s_j^{-1}s) \leq (\sum c_j)\|\varphi\|_u \quad \forall s \in G$$

whence $\sum c_j \geq \|f\|_u/\|\varphi\|_u$, and the assertion follows.

(vi) We have the implication

$$f_1 \leq \sum c_j L_{s_j} f_0 \text{ and } f_0 \leq \sum d_k L_{t_k}\varphi \quad\Rightarrow\quad f_1 \leq \sum c_j d_k L_{s_j t_k}\varphi$$

whence

$$(f_1:\varphi) \le \inf \sum c_j d_k = \inf(\sum c_j)\inf(\sum d_k) = (f_1:f_0)(f_0:\varphi)$$

as claimed. This completes the proof. ❑

The Haar covering number yields an "approximate" functional as follows. Fix $f_0 \in \mathscr{C}_c^+$ and define

$$I_\varphi(f) = \frac{(f:\varphi)}{(f_0:\varphi)} \quad (f, \varphi \in \mathscr{C}_c^+) \ .$$

By (vi) above, we have the inequalities

$$(f:\varphi) \le (f:f_0)(f_0:\varphi) \text{ and } (f_0:\varphi) \le (f_0:f)(f:\varphi) \ .$$

Dividing the first by $(f_0:\varphi)$ and the second by $(f:\varphi)$, we find that I_φ is bounded as follows:

$$(f_0:f)^{-1} \le I_\varphi(f) \le (f:f_0) \ . \tag{1.2}$$

This bound is crucial to the existence of a Haar measure for G.

One would expect that as the support of φ shrinks, I_φ will become more nearly linear. This is confirmed by the following lemma.

1-10 LEMMA. *Given f_1 and f_2 in $\mathscr{C}_c^+$, for every $\varepsilon > 0$ there is a neighborhood V of the identity e such that*

$$I_\varphi(f_1) + I_\varphi(f_2) \le I_\varphi(f_1 + f_2) + \varepsilon$$

whenever the support of φ lies in V.

PROOF. By Urysohn's lemma for locally compact Hausdorff spaces, there exists a function $g \in \mathscr{C}_c^+$ that takes the value 1 on $\text{supp}(f_1+f_2) = \text{supp}(f_1) \cup \text{supp}(f_2)$. Choose $\delta > 0$ and let $h = f_1 + f_2 + \delta g$, so that h is continuous. Next let $h_i = f_i/h$, $i=1,2$, with the understanding that h_i is 0 off the support of f_i. Clearly both h_i lie in $\mathscr{C}_c^+$, and their sum approaches 1 from below as δ tends to 0. By uniform continuity, there exists a neighborhood U of e such that $|h_i(s) - h_i(t)| < \delta$ whenever $t^{-1}s \in U$.

Assume that $\text{supp}(\varphi)$ lies in U and suppose that

$$h \le \sum_j c_j L_{s_j} \varphi \ .$$

Then

$$f_i(s) = h(s)h_i(s) \le \sum_j c_j\varphi(s_j^{-1}s)h_i(s) \le \sum_j c_j\varphi(s_j^{-1}s)(h_i(s_j)+\delta) \quad (i=1,2)$$

and it follows that

$$(f_i:\varphi) \le \sum_j c_j[h_i(s_j)+\delta] \quad (i=1,2) \ .$$

Since $h_1+h_2 \le 1$, this last inequality implies that

$$(f_1:\varphi)+(f_2:\varphi) \le (1+2\delta)\sum_j c_j \ .$$

But $\sum c_j$ may be made arbitrarily close to $(h:\varphi)$, and therefore by definition of I_φ and part (ii) of the previous lemma,

$$\begin{aligned} I_\varphi(f_1)+I_\varphi(f_2) &\le (1+2\delta)I_\varphi(h) \\ &\le (1+2\delta)[I_\varphi(f_1+f_2)+\delta I_\varphi(g)] \\ &= I_\varphi(f_1+f_2)+2\delta[I_\varphi(f_1+f_2)+\delta I_\varphi(g)] \ . \end{aligned}$$

Finally, Eq. 1.2 asserts that all of the I_φ-terms on the right are bounded independently of φ, and so for any positive $\varepsilon>0$ we can choose δ sufficiently small that the stated inequality holds. ❑

Existence of Haar Measure

We now prove the existence of a Haar measure for a locally compact group G. The idea is to construct from our approximate left-invariant functionals I_φ an exact linear functional. We shall obtain this as a limit in a suitable space.

Let X be the compact topological space defined by the bounds of $I_\varphi(f)$ as follows:

$$X = \prod_{f\in\mathscr{C}_c^+}[(f_0:f)^{-1},(f:f_0)] \ .$$

Then every function I_φ (in the technical sense of a set of ordered pairs in $\mathscr{C}_c^+ \times \mathbf{R}_+^*$) lies in X. For every compact neighborhood U of e, let K_U be the closure of the set $\{I_\varphi : \mathrm{supp}(\varphi) \subseteq U\}$ in X. The collection $\{K_U\}$ satisfies the finite intersection property, since

$$\bigcap_{j=1}^n K_{U_j} \supseteq K_{\bigcap_{j=1}^n U_j}$$

and the right side is nonempty by Urysohn's lemma. Therefore, since X is compact, $\bigcap K_U$ contains an element I, which will in fact extend to the required left-invariant positive linear functional on $\mathscr{C}_c(G)$. Note that I, which lies in a product of closed intervals excluding zero, cannot be the zero function on $\mathscr{C}_c(G)$, so that the extended functional will likewise be nontrivial.

Since I is in the intersection of the closure of the sets $\{I_\varphi : \text{supp}(\varphi) \subseteq U\}$, it follows that every open neighborhood of I in the product X intersects each of the sets $\{I_\varphi : \text{supp}(\varphi) \subseteq U\}$. We may unwind this assertion as follows:

> For every open neighborhood U of e, and for every trio of functions $f_1, f_2, f_3 \in \mathscr{C}_c^+$ and every $\varepsilon > 0$, there exists a function $\varphi \in \mathscr{C}_c^+$ with $\text{supp}(\varphi) \subseteq U$ such that $|I(f_j) - I_\varphi(f_j)| < \varepsilon, j = 1,2,3$.

(This statement extends to any finite collection of f_j, but we shall need only three.) So given $f \in \mathscr{C}_c^+$ and $c \in \mathbf{R}$, we may simultaneously make $I(cf)$ arbitrarily close to $I_\varphi(cf)$ and $cI(f)$ arbitrarily close to $cI_\varphi(f)$. Appealing to Lemma 1-9 above, this shows that $I(cf) = cI(f)$. Similarly we have that I is left translation-invariant and at least subadditive. To see that I is in fact additive, we use Lemma 1-10 to choose a neighborhood U of e such that

$$I_\varphi(f_1) + I_\varphi(f_2) \leq I_\varphi(f_1 + f_2) + \frac{\varepsilon}{4}$$

whenever $\text{supp}(\varphi) \subseteq U$. Then choose φ with $\text{supp}(\varphi) \subseteq U$ such that $I(f_1)$, $I(f_2)$, and $I(f_1 + f_2)$ all likewise lie within $\varepsilon/4$ of $I_\varphi(f_1)$, $I_\varphi(f_2)$, and $I_\varphi(f_1 + f_2)$, respectively. Since ε is arbitrary, it follows at once from the inequality above and the general sublinearity of I_φ that $I(f_1 + f_2) = I(f_1) + I(f_2)$, as required.

Finally, extend I to a positive left translation-invariant linear functional on $\mathscr{C}_c(G)$ by setting $I(f) = I(f^+) - I(f^-)$. As we remarked above, in view of our general discussion of translation-invariant measures and the Riesz representation theorem, this implies that G admits a left Haar measure μ and completes the existence proof. ❑

Uniqueness of Haar Measure

We now prove that the Haar measure on a locally compact group G is unique up to a positive scalar multiple. Given two Haar measures μ and ν on G, clearly it suffices to show that the ratio of integrals

$$\frac{\int_G f(x)\,d\mu}{\int_G f(x)\,d\nu}$$

is independent of $f \in \mathscr{C}_c^+$. To simplify the notation, we shall often write $I(f)$ and $J(f)$ for the indicated integrals with respect to μ and ν, respectively. Given two functions $f, g \in \mathscr{C}_c^+$, the plan is to produce a function $h \in \mathscr{C}_c^+$ such that the ratios $I(f)/J(f)$ and $I(g)/J(g)$ can both be made arbitrarily close to $I(h)/J(h)$.

Let K be a compact subset of G, the interior of which contains e. Then K contains an open symmetric neighborhood of the identity whose closure K_0 is compact and symmetric. (The symmetry is clearly preserved by closure.) Define compact subsets K_f and K_g of G by

$$K_f = \mathrm{supp}(f)\cdot K_0 \cup K_0\cdot \mathrm{supp}(f) \quad \text{and} \quad K_g = \mathrm{supp}(g)\cdot K_0 \cup K_0\cdot \mathrm{supp}(g)\ .$$

(Recall that the group product of compact sets is compact.) For $t \in K_0$, define $\gamma_t f$ by

$$\gamma_t f(s) = f(st) - f(ts)\ .$$

Equivalently, we have

$$\gamma_t f = R_t f - L_{t^{-1}} f\ .$$

Define $\gamma_t g$ similarly. Clearly $\gamma_t f$ and $\gamma_t g$ are supported in K_f and K_g, respectively, and both vanish on the center of G and in particular at e. Let $\varepsilon > 0$ be given. Then by left and right uniform continuity, K_0 contains an open neighborhood U_0 of e such that for all $s \in G$ and $t \in U_0$, both $|\gamma_t f(s)|$ and $|\gamma_t g(s)|$ are bounded by $\varepsilon/2$. Now U_0 in turn contains a symmetric open neighborhood U_1 of e whose closure K_1 is symmetric, compact, and contained in K_0. Moreover, by continuity we have that $|\gamma_t f(s)| < \varepsilon$ and $|\gamma_t g(s)| < \varepsilon$ for all $s \in G$ and all $t \in K_1$. The point is that as long as t remains in K_1, translation of f and g by t on either side has approximately the same effect.

We now construct h. We claim first that since e lies in the interior of K_1, there exists a second compact neighborhood K_2 of e such that K_2 is contained in the interior of K_1. Granting this, it follows immediately from Urysohn's lemma for locally compact topological spaces that there exists a continuous function $\tilde{h}: G \to \mathbf{R}_+$ that is 1 on K_2 and 0 outside of K_1. Define $h: G \to \mathbf{R}_+$ by

$$h(s) = \tilde{h}(s) + \tilde{h}(s^{-1})\ .$$

Then certainly $h \in \mathscr{C}_c^+$, supp(h) lies in K_1, and h is an even function in the sense that $h(s) = h(s^{-1})$.

Proof of Claim. Since G is Hausdorff and the boundary B of K_1 is likewise compact, B admits a finite cover by open sets each of which is disjoint from a corresponding open neighborhood of e in K_1. The intersection of these neighborhoods thus constitutes an open neighborhood U_2 of e in K_1, and we now set K_2 equal to the closure of U_2. Then by construction K_2 is contained in the interior of K_1, as required. ❑

We come to the main calculations. All integrals are implicitly over G and are translation-invariant, since μ and ν are by assumption Haar measures. First,

$$\begin{aligned} I(f)J(h) &= \iint f(s)h(t)\,d\mu_s d\nu_t \\ &= \iint f(ts)h(t)\,d\mu_s d\nu_t \ . \end{aligned}$$

The second calculation uses the property that h is even.

$$\begin{aligned} I(h)J(f) &= \iint h(s)f(t)\,d\mu_s d\nu_t \\ &= \iint h(t^{-1}s)f(t)\,d\mu_s d\nu_t \\ &= \iint h(s^{-1}t)f(t)\,d\mu_s d\nu_t \\ &= \iint h(t)f(st)\,d\mu_s d\nu_t \ . \end{aligned}$$

From these we can easily estimate the difference:

$$\begin{aligned} |I(h)J(f) - I(f)J(h)| &= \left| \iint h(t)\{f(st) - f(ts)\}\,d\mu_s d\nu_t \right| \\ &= \left| \iint h(t)\gamma_t f(s)\,d\mu_s d\nu_t \right| \\ &\leq \varepsilon\mu(K_f)J(h) \ . \end{aligned}$$

The point in the last line of the calculation is that supp(h) lies in a K_1 where $\gamma_t f$ is small. Similarly,

$$\begin{aligned} |I(h)J(g) - I(g)J(h)| &= \left| \iint h(t)\{g(st) - g(ts)\}\,d\mu_s d\nu_t \right| \\ &= \left| \iint h(t)\gamma_t g(s)\,d\mu_s d\nu_t \right| \\ &\leq \varepsilon\mu(K_g)J(h) \ . \end{aligned}$$

Dividing the first inequality by $J(h)J(f)$ yields

$$\left| \frac{I(h)}{J(h)} - \frac{I(f)}{J(f)} \right| \leq \frac{\varepsilon\mu(K_f)}{J(f)} \ .$$

Dividing the second by $J(h)J(g)$ yields

$$\left| \frac{I(h)}{J(h)} - \frac{I(g)}{J(g)} \right| \leq \frac{\varepsilon\mu(K_g)}{J(g)} \ .$$

Since ε is arbitrary, this shows that the ratio $I(f)/J(f)$ is independent of f as claimed. ❑

1.3 Profinite Groups

This section introduces a special class of topological groups of utmost importance to our subsequent work. We begin by establishing a categorical framework for the key definition that follows.

Projective Systems and Projective Limits

Let I be a nonempty set, which shall later serve as a set of indices. We say that I is *preordered* with respect to the relation $\leq$ if the given relation is reflexive (i.e., $i \leq i$ for all $i \in I$) and transitive (i.e., $i \leq j$ and $j \leq k \Rightarrow i \leq k$ for all $i, j, k \in I$). Note that we do not assume antisymmetry (i.e., $i \leq j$ and $j \leq i$ need not imply that $i = j$); hence a preordering is weaker than a partial ordering. Clearly the elements of a preordered set I constitute the objects of a category for which there is a unique morphism connecting two elements i and j if and only if $i \leq j$.

We say that a preordered set I is moreover a *directed set* if every finite subset of I has an upper bound in I; equivalently, for all $i, j \in I$ there exists $k \in I$ such that $i \leq k$ and $j \leq k$. (Recall that directed sets are precisely what is needed to define the notion of a net in an abstract topological space.) While most of the specific instances of preordered sets that we meet below will moreover be directed, we shall need only the preordering for the general categorical constructions to follow. Beware, however, that directed sets will play a crucial but subtle role in establishing that the projective limit of nonempty sets is itself nonempty. (See Proposition 1-11.)

EXAMPLE. The integers **Z** are preordered (but not partially ordered) with respect to divisibility and in fact constitute a directed set: a finite collection of integers is bounded with respect to divisibility by its least common multiple.

Assume that I is a preordered set of indices and let $\{G_i\}_{i \in I}$ be a family of sets. Assume further that for every pair of indices $i, j \in I$ with $i \leq j$ we have an associated mapping $\varphi_{ij} : G_j \to G_i$, subject to the following conditions:

(i) $\varphi_{ii} = 1_{G_i} \quad \forall i \in I$

(ii) $\varphi_{ij} \circ \varphi_{jk} = \varphi_{ik} \quad \forall i, j, k \in I, i \leq j \leq k$

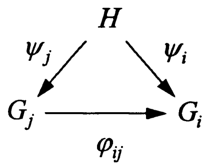
Then the system (G_i, φ_{ij}) is called a *projective* (or *inverse*) *system*. Note that if we regard I as a category, then the association $i \mapsto G_i$ defines a contravariant functor.

DEFINITION. Let (G_i, φ_{ij}) be a projective system of sets. Then we define the *projective limit* (or *inverse limit*) of the system, denoted $\varprojlim G_i$, by

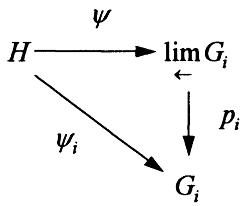
$$\varprojlim G_i = \{(g_i) \in \prod_{i \in I} G_i : i \leq j \Rightarrow \varphi_{ij}(g_j) = g_i\} .$$

Note that as a subset of the direct product, $\varprojlim G_i$ comes naturally equipped with a family of projection maps $p_j : \varprojlim G_i \to G_j$, and with regard to these projections, the projective limit manifests the following universal property:

UNIVERSAL PROPERTY. *Let H be a nonempty set and let there be given a system of maps $(\psi_i : H \to G_i)_{i \in I}$ that is compatible with the projective system (G_i, φ_{ij}) in the sense that for each pair of indices $i, j \in I$ with $i \leq j$, the following diagram commutes:*



Then there exists a unique map $\psi : H \to \varprojlim G_i$ such that for each $i \in I$ the diagram



also commutes.

The mapping ψ is of course none other than $h \mapsto (\psi_i(h))_{i \in I}$, just as for the direct product of sets, but in this case the compatibility of the ψ_i guarantees that the image falls into the projective limit.

Note carefully that neither the definition of a projective limit nor the associated universal property asserts that a given projective limit of sets is nonempty. In particular, the projection maps may have empty domain. Of course, if a compatible system $(\psi_i : H \to G_i)_{i \in I}$ exists with nonempty domain H, then one infers from the existence of elements of the form $(\psi_i(h))_{i \in I}$ that the projective limit is likewise nonempty.

The construction of the projective limit works equally well in the category of groups (in which case the set maps are replaced by group homomorphisms, and

the group operation is defined componentwise) or the category of topological spaces (in which case the set maps must be replaced by continuous functions, and the topology on the projective limit is the subspace product topology induced from the direct product). In the case of groups, note that the projective limit is never empty, since the identity element of the direct product clearly lies in the projective limit. It follows from these remarks that the projective limit of a projective system of topological groups is itself a topological group with respect to the componentwise multiplication and the subspace topology.

REMARK. A more obvious topology on a product space $\prod X_i$ is the *box topology*, generated by sets of the form $\prod U_i$ with U_i open in X_i for all i. But this is a much finer topology than the standard product topology. Moreover, with respect to the box topology the product of compact spaces need not be compact.

In the following subsection we shall be concerned with projective limits of finite groups. In passing we shall require conditions under which the projective limit of finite sets is nonempty. It is here that the notion of a directed set reappears critically.

1-11 PROPOSITION. *Assume that I is a directed set, and let (G_i, φ_{ij}) be a projective system of finite sets. Set $G = \varprojlim G_i$. Then:*

(i) *If each G_i is nonempty, G is nonempty.*

(ii) *For each index $i \in I$,*

$$p_i(G) = \bigcap_{i \le j} \varphi_{ij}(G_j) \quad .$$

PROOF. Our proof is adapted from a more general result in Bourbaki's *Theory of Sets*, Chapter III, § 7.4. Let us call $(S_i)_{i \in I}$ a *compatible family* (with respect to our given projective system) if the following conditions are satisfied:

(a) For all $i \in I$, $S_i \subseteq G_i$.

(b) For all $i, j \in I$ with $i \le j$, $\varphi_{ij}(S_j) \subseteq S_i$.

(c) For all $i \in I$, $S_i \ne \varnothing$.

Note well that if (S_i) is a compatible family of the form $S_i = \{x_i\}$ for all $i \in I$, then in fact $(x_i) \in G$, which in this case is *ipso facto* nonempty.

Henceforth let Σ denote the set of all compatible families. We impose an ordering on Σ as follows: given compatible families (S_i) and (T_i), we shall write $(S_i) \le (T_i)$ if $S_i \supseteq T_i$ for all i. If Σ' is a totally ordered subset of Σ, then clearly Σ' admits the upper bound (T_i) defined by

$$T_i = \bigcap_{(S_j)\in\Sigma'} S_i \ .$$

Conditions (a)–(c) are trivially satisfied, and only the last of these requires finiteness. Hence the given ordering is inductive.

Suppose that there exists a maximal compatible system $(S_i)\in\Sigma$. We claim that $S_i = \varphi_{ij}(S_j)$ for all $i \le j$. To prove this, let (T_i) be defined by

$$T_i = \bigcap_{i\le j} \varphi_{ij}(S_j) \subseteq S_i \ .$$

Since (S_i) is assumed maximal, our claim is established, provided that we can show that also $(T_i)\in\Sigma$. Again (a) and (b) are routine; (c) is interesting. First observe that if $i \le j \le k$, then $\varphi_{ik}(S_k) \subseteq \varphi_{ij}(S_j)$. Now consider the intersection that defines T_i. Each of the factors appearing is a subset of the finite set S_i. There are only finitely many such subsets, and consequently we may assume that the intersection is over a finite set of indices $j_1,\ldots,j_r$. *But I is directed, so there exists an element k in I such that* $k \ge j_1,\ldots,j_r$. Thus by our previous observation,

$$\varphi_{ik}(S_k) \subseteq \bigcap_{m=1}^{r} \varphi_{ij_m}(S_{j_m}) = T_i$$

and therefore T_i is manifestly nonempty.

We continue to assume that (S_i) is maximal in Σ and shall demonstrate next that each S_i contains exactly one element. Fix i and let $x_i \in S_i$. Define (T_j) as follows:

$$T_j = \begin{cases} S_j \cap \varphi_{ij}^{-1}(x_i) & \text{if } i \le j \\ S_j & \text{otherwise.} \end{cases}$$

Note in particular that $T_i = \{x_i\}$, since φ_{ii} is the identity on S_i. Then (T_j) lies in Σ: (a) is obvious, (b) is an easy exercise, and (c) follows from the claim of the previous paragraph, namely that $S_i = \varphi_{ij}(S_j)$ for all $j \ge i$. Moreover, by construction $(S_j) \le (T_j)$, whence, since (S_j) is maximal, we must in fact have equality. This shows that $S_i = \{x_i\}$. Since i was arbitrary, this suffices.

We now address both statements of the proposition. Again fix $i \in I$. By definition of a projective system,

$$p_i(G) \subseteq \bigcap_{i\le j} \varphi_{ij}(G_j) \ .$$

One may argue as above that since all but finitely many factors on the right are redundant, the given intersection is nonempty; thus it contains an element x_i. Define (T_j) as follows:

$$T_j = \begin{cases} \varphi_{ij}^{-1}(x_i) & \text{if } i \leq j \\ G_j & \text{otherwise.} \end{cases}$$

Note in particular that $T_i = \{x_i\}$. One sees without difficulty that $(T_j) \in \Sigma$ (at last establishing that Σ is nonempty!), and so by Zorn's lemma there is a maximal element (S_j) of Σ with the additional property that $(S_j) \geq (T_j)$. But then $(S_j) = \{y_j\}$ and G is nonempty, as required by (i). Moreover, $x_i = y_i \in p_i(G)$, which in light of the preceding inclusion establishes (ii). ❑

Profinite Groups

We now come to the principal definition of this section. It may seem at first to be essentially group-theoretic, with the topology as an afterthought, but we shall see shortly that this is not the case.

Consider a projective system of finite groups, each of which we take as having the discrete topology. Their projective limit acquires the relative topology induced by the product topology on the full direct product. This is called the *profinite topology*, and accordingly the projective limit acquires the structure of a topological group.

DEFINITION. A topological group isomorphic to the projective limit of a projective system of finite groups (endowed with the profinite topology) is called a *profinite group*.

The following proposition summarizes the most fundamental global properties of a profinite group.

1-12 PROPOSITION. *Let G be a profinite group, given as the projective limit of the projective system (G_i, φ_{ij}). Then the following assertions hold:*

(i) *G is Hausdorff with respect to the profinite topology.*

(ii) *G is a closed subset of the direct product $\prod G_i$.*

(iii) *G is compact.*

PROOF. (i) The direct product of Hausdorff spaces is also Hausdorff, and any subset of a Hausdorff space is clearly also Hausdorff in the induced topology.

(ii) We may realize the complement of G in $\prod G_i$ as an open set as follows:

$$G^c = \bigcup_i \bigcup_{j \geq i} \{(g_k) \in \prod G_k : \varphi_{ij}(g_j) \neq g_i\} \ .$$

Therefore G is closed, as claimed.

(iii) Since the direct product $\prod G_i$ is compact by Tychonoff's theorem, this assertion follows from (ii) on general principles: a closed subset of a compact space is itself compact. ❑

EXAMPLES

(1) Let $G_n = \mathbf{Z}/n\mathbf{Z}$, $n \geq 1$, the additive group of integers modulo n. Then $\{G_n\}$ is a projective system, since there is a canonical projection

$$\begin{aligned} \varphi_{mn} : \mathbf{Z}/n\mathbf{Z} &\to \mathbf{Z}/m\mathbf{Z} \\ [k]_n &\mapsto [k]_m \end{aligned}$$

whenever $m \mid n$, and these projections are clearly compatible in the required sense. We may thus form their projective limit

$$\hat{\mathbf{Z}} = \lim_{\leftarrow} \mathbf{Z}/n\mathbf{Z} \ .$$

Note that $\hat{\mathbf{Z}}$ also admits the structure of a topological ring.

(2) Let $H_n = (\mathbf{Z}/n\mathbf{Z})^\times$, $n \geq 1$, the group of units in $\mathbf{Z}/n\mathbf{Z}$. Then $\{H_n\}$ is a projective system, since a (unital) ring homomorphism maps units to units. Set

$$\hat{\mathbf{Z}}^\times = \lim_{\leftarrow} (\mathbf{Z}/n\mathbf{Z})^\times \ .$$

Then $\hat{\mathbf{Z}}^\times$ is a topological group under multiplication and in fact is the group of units of $\hat{\mathbf{Z}}$.

(3) Fix a rational prime p and set $G_m = \mathbf{Z}/p^m\mathbf{Z}$, $m \geq 1$. Again $\{G_m\}$ is a projective system, and we form its projective limit to obtain a ring

$$\mathbf{Z}_p = \lim_{\leftarrow} \mathbf{Z}/p^m\mathbf{Z} \ .$$

This is called *the ring of p-adic integers.*

(4) Let $H_m = (\mathbf{Z}/p^m\mathbf{Z})^\times$, $m \geq 1$, so that $\{H_m\}$ is a projective system as in Example 2. Then set

$$\mathbf{Z}_p^\times = \varprojlim (\mathbf{Z}/p^m\mathbf{Z})^\times \ .$$

One checks easily that $\mathbf{Z}_p^\times$ is the group of units in $\mathbf{Z}_p$; this is called *the group of p-adic units.*

(5) The set of all finite Galois extensions $K/\mathbf{Q}$ within a fixed algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$ forms a directed set with respect to inclusion. We have a corresponding directed system of finite groups $\mathrm{Gal}(K/\mathbf{Q})$, where if $K \subseteq L$, the associated homomorphism $\mathrm{Gal}(L/\mathbf{Q}) \to \mathrm{Gal}(K/\mathbf{Q})$ is just restriction. Moreover, we have an isomorphism

$$\begin{aligned} \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) &\xrightarrow{\approx} \varprojlim \mathrm{Gal}(K/\mathbf{Q}) \\ \sigma &\mapsto (\sigma|_K) \ . \end{aligned}$$

Topological Characterization of Profinite Groups

Recall that a topological space X is called *connected* if whenever $X = U \cup V$ for nonempty open subsets U and V, then $U \cap V \neq \varnothing$. (Evidently an equivalent statement results if we substitute nonempty closed subsets for open ones.) Every point $x \in X$ is contained in a maximal connected subset of X, which is called the *connected component* of x. In the special case of a topological group G, the connected component of the identity e is denoted G°.

A topological space X is called *totally disconnected* if every point in X is its own connected component. Clearly a homogeneous space is totally disconnected if and only if some point is its own connected component. In particular, a topological group G is totally disconnected if and only if $G^\circ = \{e\}$.

1-13 LEMMA. *G° is a normal subgroup of G. Moreover, the quotient space G/G° is totally disconnected, whence $(G/G^\circ)^\circ$ is the trivial subgroup of the quotient.*

PROOF. Let $x \in G^\circ$. Then $x^{-1}G^\circ$ is connected (by homogeneity) and contains e, whence $x^{-1}G^\circ \subseteq G^\circ$. Thus G° is closed under inverses. The same argument now shows that $xG^\circ \subseteq G^\circ$, and that for all $y \in G$, we have further that $yG^\circ y^{-1} \subseteq G^\circ$. Consequently G° is indeed a normal subgroup of G°, as claimed. The second statement is immediate: by homogeneity, the connected components of G are precisely the elements of G/G°, and so by general topology (see Exercise 5 below), G/G° is totally disconnected. ❑

1-14 THEOREM. *Let G be a topological group. Then G is profinite if and only if G is compact and totally disconnected.*

PROOF. $\Rightarrow$) We have already seen that G is compact. Thus it remains to show that $G^\circ = \{e\}$. Let U be any open subgroup of G. Then $U \cap G^\circ$ is open in G° and nonempty. Now consider the subset V of G defined by

$$V = \dot{\bigcup_{x \in G^\circ - U}} x \cdot (U \cap G^\circ) .$$

Then since each $x \cdot (U \cap G^\circ)$ is open in G°, so is V. Moreover, by elementary group theory, $U \cap V = \varnothing$, and G° is the disjoint union of two open sets, namely $U \cap G^\circ$ and V. But by definition G° is connected, so either $U \cap G^\circ$ or V must be empty. Since the former is not, the latter is, and in fact $G^\circ = U \cap G^\circ$, which is to say that $G^\circ \subseteq U$. Since U is an arbitrary open subgroup of G, we have accordingly,

$$G^\circ \subseteq \bigcap_{\substack{U \text{ an open} \\ \text{subgroup of } G}} U .$$

We must now make use of the profinite nature of G. Indeed, let

$$G = \lim_{\leftarrow} G_i$$

where each G_i is a finite group with the discrete topology. Recall that for each index i we have a projection map $p_i : G \to G_i$ that is just the restriction of the corresponding map on the full direct product. Let $y = (y_i)$ lie in G and assume that y is not the identity element. Then for some index i_0, it must be the case that $y_{i_0} \neq e_{i_0}$. But now consider the set $U_0 = p_{i_0}^{-1}(e_i)$. Since the topology on G_{i_0} is discrete and the projections are continuous, U_0 is open in G. Since the projections are moreover group homomorphisms, U_0 is in fact a subgroup of G. But by construction, U_0 excludes y. This shows that the only element in the intersection of all open subgroups of G is the identity. Thus G° is trivial, as required.

The proof of the converse is more delicate and requires three lemmas. We begin with some preliminary analysis.

Let $\mathcal{N}$ be the family of open, normal subgroups of G. This is clearly a directed set with respect to the relation $M \leq N$ if $N \subseteq M$. (In fact, two subgroups M and N in $\mathcal{N}$ have a least upper bound $M \cap N$ in $\mathcal{N}$.) Moreover, the following observations are elementary:

(i) For each $N \in \mathcal{N}$, the quotient group G/N is both compact and discrete, hence finite.

(ii) For each pair of subgroups $M,N \in \mathcal{N}$, with $M \leq N$, the kernel of the canonical projection $G \rightarrow G/M$ contains N, and hence this map factors through G/N to yield the induced map

$$\begin{aligned} \varphi_{M,N}: G/N &\rightarrow G/M \\ xN &\mapsto xM \end{aligned} .$$

From this description it is clear that if $L \leq M \leq N$ in $\mathcal{N}$, then

$$\varphi_{L,M} \circ \varphi_{M,N} = \varphi_{L,N}$$

and $\{G/N\}_{N \in \mathcal{N}}$ constitutes a projective system of finite groups.

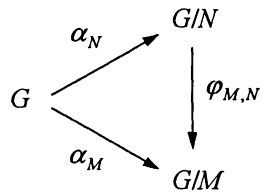
The point, of course, is to show that G is isomorphic to the projective limit of this system.

1-15 LEMMA. *Let the profinite group G' be given by*

$$G' = \lim_{\substack{\leftarrow \\ N}} G/N$$

where N varies over $\mathcal{N}$, as defined above. Then there exists a surjective, continuous homomorphism $\alpha: G \rightarrow G'$.

PROOF. For $N \in \mathcal{N}$ let α_N denote the canonical projection from G to G/N, which is surjective. Since G/N is homogeneous, we establish that α_N is also continuous by noting that $\alpha_N^{-1}(e_{G/N}) = N$, which by hypothesis is open in G. Arguing as in (ii) above, it is clear that whenever $M \leq N$ in $\mathcal{N}$, the following triangle is commutative:



Thus by the universal property of projective limits, we have a continuous homomorphism $\alpha: G \rightarrow G'$ such that $\alpha_N = p_N \circ \alpha$ for all $N \in \mathcal{N}$, where p_N denotes projection from G' onto G/N, the component of the projective limit corresponding to N.

It remains to show that α is surjective. We claim that α has dense image in G'. Granting this, we conclude the argument as follows: Since G is compact

and G' is Hausdorff, the image of α is, moreover, closed in G'. Thus $\mathrm{Im}(\alpha)$, being dense, must be all of G', as required.

To establish the claim we shall show that no open subset of G' is disjoint from $\mathrm{Im}(\alpha)$. Consider the topology of G': this is generated by sets of the form $p_N^{-1}(S_N)$, where S_N is an arbitrary subset of G/N. Every open set in G' is thus expressible as a union of finite intersections of these $p_N^{-1}(S_N)$. Such an intersection U consists of elements of the form

$$(\overline{x}_N)_{N\in\mathcal{N}}$$

where at most only finitely many of the coordinates are constrained to lie in some given proper subset of the corresponding quotient; the rest are unrestricted. Now suppose that the constrained coordinates correspond to the subgroups $N_1,\ldots,N_r$ and that

$$M=\bigcap_{j=1}^{r} N_j\ .$$

Then given $(x_N)\in G'$, the coordinates x_{N_j} are all determined as images of the coordinate x_M under the associated projection maps. Since $\alpha_M: G\to G/M$ is surjective, there is at least one element in $t\in G$ such that $\alpha(t)_M=x_M$, and consequently t also satisfies $\alpha(t)_{N_j}=x_{N_j}$ for $j=1,\ldots,r$. In particular, if $(x_N)\in U$, then certainly $\alpha(t)\in U$, since $\alpha(t)$ agrees with (x_N) in all of the constrained coordinates. Thus U manifestly intersects $\mathrm{Im}(\alpha)$, and by our previous remarks, so, too, does every open set in G'. This completes the proof. ❑

1-16 LEMMA. *Let X be a compact Hausdorff space. For a fixed point $P\in X$, set* $\mathcal{U}=\{K:K$ is a compact, open neighborhood of $P\}$. *Define $Y\subseteq X$ by*

$$Y=\bigcap_{K\in\mathcal{U}} K\ .$$

Then Y is connected.

PROOF. Note that the collection $\mathcal{U}$ is nonempty because X itself is compact and open.

Suppose that Y is the disjoint union of closed subsets Y_1 and Y_2. We must show that either Y_1 or Y_2 is empty. Recall from general topology that a compact Hausdorff space is normal. Accordingly, there exist disjoint open subsets U_1 and U_2 containing, respectively, Y_1 and Y_2. Now set $Z=X-(U_1\cup U_2)$, which is closed and therefore compact. Since $Y\subseteq U_1\cup U_2$, Z and Y are disjoint, which is to say that Z lies in the complement of Y. Thus we have an open cover for Z

$$Z \subseteq \bigcup_{K \in \mathcal{U}} K^c$$

that admits a finite subcover. Hence there exist $K_1,\ldots,K_r \in \mathcal{U}$ such that

$$Z \cap (\bigcap_j K_j) = \varnothing \ .$$

Let W denote the intersection of the K_j. Then W is a compact, open neighborhood of P, and so W is itself in $\mathcal{U}$. But also

$$W = (W \cap U_1) \ \dot{\cup} \ (W \cap U_2)$$

since W is disjoint from Z, the complement of $U_1 \cup U_2$. We now make note of the following assertions:

(i) Both $W \cap U_1$ and $W \cap U_2$ are compact, open subsets of X.

(ii) P lies exclusively in one of $W \cap U_1$ or $W \cap U_2$. Say $P \in W \cap U_1$.

From (i) and (ii) it follows that $W \cap U_1 \in \mathcal{U}$ and so $Y \subseteq W \cap U_1$. Since $Y_2 \subseteq Y$ and Y_2 is disjoint from U_1, it follows that Y_2 is empty, as required. ❑

1-17 LEMMA. *Let G be a compact, totally disconnected topological group. Then every neighborhood of the identity contains an open normal subgroup.*

PROOF. As a preliminary, note that G is Hausdorff: If x and y are distinct points in G, then $\{x,y\}$ is disconnected with respect to the subspace topology. Therefore there exist respective open neighborhoods of x and y that are disjoint. The proof now proceeds in three steps: First, we show that every open neighborhood U of the identity contains a compact, open neighborhood W of the identity. Second, we show that W in turn contains an open, symmetric neighborhood V of the identity such that $WV \subseteq W$. Third, from V we construct an open subgroup, then an open, normal subgroup of G contained in U, as required.

Let $\mathcal{U}$ denote the set of all compact, open neighborhoods of the group identity e. Applying the previous lemma with $P=e$, we find that

$$Y = \bigcap_{K \in \mathcal{U}} K$$

is a connected set containing e. But G is totally disconnected, so in fact $Y=\{e\}$. Now let U denote any open neighborhood of e. Then $G-U$ is closed and therefore compact. Since e is the only element of G common to all of the K in

$\mathscr{U}$, there exist subsets $K_1,\ldots,K_r \in \mathscr{U}$ whose complements cover $G-U$, and therefore

$$W = \bigcap_{j=1}^{r} K_j$$

is a subset of U and a compact, open neighborhood of e. In particular, $W \in \mathscr{U}$. This completes the first step.

To begin the second step, consider the continuous map $\mu: W \times W \to G$ defined by restriction of the group operation. We make the following observations:

(i) For every $w \in W$, the point $(w,e) \in \mu^{-1}(W)$.

(ii) Since W is open, the inverse image of W itself under μ is open in $W \times W$.

(iii) It follows from (i) and (ii) that for every $w \in W$, there exists open neighborhoods U_w of w and V_w of e such that $U_w \times V_w \subseteq \mu^{-1}(W)$. Moreover, by Proposition 1-1, we may assume that each V_w is symmetric.

(iv) The collection of subsets U_w $(w \in W)$ constitutes an open cover for W. Since W is compact, a finite subcollection $U_1,\ldots,U_r$ suffices.

Let $V_1,\ldots,V_r$ correspond to $U_1,\ldots,U_r$ in (iii) above. Define an open neighborhood $V \subseteq W$ of the identity as follows:

$$V = \bigcap_{j=1}^{r} V_j \ .$$

By construction $WV \subseteq W$, and by induction $WV^n \subseteq W$ for all $n \geq 0$. In particular, $V^n \subseteq W$ for all $n \geq 0$. This completes the second step.

For the final step, we expand V to an open subgroup O of G contained in W by the formula

$$O = \bigcup_{n=1}^{\infty} V^n \ .$$

(Note that O is closed under inversion because V is symmetric.) The quotient space G/O is compact and discrete, hence finite, so we can find a finite collection of coset representatives $x_1,\ldots,x_s$ for O in G. It follows that O likewise has only finitely many conjugates in G: all take the form

$$x_j O x_j^{-1} \qquad (j = 1,\ldots,s) .$$

Thus

$$N = \bigcap_{j=1}^{s} x_j O x_j^{-1}$$

is an open, normal subgroup of G. Moreover, since one of the conjugates of O is O itself, $N \subseteq O \subseteq W \subseteq U$. This completes the proof. ❑

This brings us at last to the conclusion of the topological characterization of profinite groups.

PROOF OF THEOREM 1-14, CONVERSE. By Lemma 1-15, we have a surjective homomorphism $\alpha: G \to G'$, where G' is the projective limit of the finite quotients G/N for N an open, normal subgroup of G (i.e., $N \in \mathcal{N}$). Appealing to Exercise 9 below, we see that it suffices to show that α has trivial kernel and hence is injective.

Since α simultaneously projects on all of the quotients, it is clear that

$$\operatorname{Ker}(\alpha) = \bigcap_{N \in \mathcal{N}} N \ .$$

By the previous lemma, every open neighborhood of $e \in G$ contains an open, normal subgroup, which is therefore represented in the intersection above. It follows that $\operatorname{Ker}(\alpha)$ is contained in *every* neighborhood of e and hence in the intersection of all such neighborhoods. But G is Hausdorff: the intersection of all neighborhoods of e consists merely of e itself. Hence $\operatorname{Ker}(\alpha)$ is indeed trivial, and the theorem is proved. ❑

The Structure of Profinite Groups

The following theorem shows in particular that closed subgroups of profinite groups and profinite quotients by closed normal subgroups are likewise profinite.

1-18 THEOREM. *Let G be a profinite group and let H be a subgroup of G. Then H is open if and only if G/H is finite. Moreover, the following three statements are equivalent.*

(i) *H is closed.*

(ii) *H is profinite.*

(iii) *H is the intersection of a family of open subgroups.*

Finally, if (i)–(iii) *are satisfied, then G/H is compact and totally disconnected.*

PROOF. The first statement follows from Proposition 1-4, part (iv), since a profinite group is necessarily compact. We next establish the given equivalences.

(i)⇒(ii) H is a closed subset of a compact space and therefore itself compact. Hence it remains to show that H is totally disconnected. But this is trivial: since $G^\circ=\{e\}$, also $H^\circ=\{e\}$, and this suffices by homogeneity.

(ii)⇒(i) If H is itself profinite, it is a compact subset of a Hausdorff space and hence closed.

(iii)⇒(i) Suppose that H is the intersection of some family of open subgroups of G. Then since every open subgroup is also closed [Proposition 1-1, part (iv)], H is also the intersection of a family of closed subgroups of G, and therefore itself closed.

(i)⇒(iii) As above, let $\mathcal{N}$ denote the family of all open, normal subgroups of G. If $N\in\mathcal{N}$, then since N is normal, NH is a subgroup of G. By part (i), $[G:N]$ is finite, whence $[G:NH]$ is likewise finite and NH is open. Moreover, clearly

$$H\subseteq \bigcap_{N\in\mathcal{N}} NH \ .$$

It remains only to demonstrate the opposite inclusion. So let x lie in the indicated intersection, and let U be any neighborhood of x. Then Ux^{-1} is a neighborhood of e, and so by Lemma 1-16, Ux^{-1} contains some $N_0\in\mathcal{N}$. Since x lies in the given intersection, $x\in N_0H$. Now by construction, also $x\in N_0x$. Hence N_0x is equal to N_0h for some $h\in H$, and consequently $h\in N_0x\subseteq U$. The upshot is that every neighborhood of x intersects H, and hence x lies in the closure of H. But H is closed by hypothesis, and therefore $x\in H$, as required.

For the final statement, the compactness of the quotient follows at once from the compactness of G. Let $\rho: G\to G/H$ denote the canonical map. To see that G/H is totally disconnected, assume that $\rho(X)$ is a connected subset of G/H that properly contains $\rho(H)$. Then $Y=X-H$ is nonempty, and since we may assume that H is nontrivial, Y contains more than one point. Hence Y is the disjoint union of nonempty open (hence closed) sets F_1 and F_2. One checks easily that since H is closed, F_1 and F_2 are both open (hence closed) in X. Thus X is the disjoint union of the two nonempty closed sets $F_1\cup H$ and F_2. But then the image of F_2 under ρ is (a) nonempty, (b) not the full image of X, and (c) both open and closed in $\rho(X)$. Since $\rho(X)$ is connected, this is a contradiction. Hence the connected component of $\rho(H)$ is $\rho(H)$ itself, and the quotient is totally disconnected, as claimed. ❑

A Little Galois Theory

We close this section by showing how profinite groups make a momentous appearance in connection with the Galois theory of infinite extensions. To begin, we recall the following elements of field theory:

(i) Let F be a field. An element a that is algebraic over F is called *separable* if the irreducible polynomial of a over F has no repeated roots. An algebraic field extension K/F is called *separable* if every element of K is separable over F.

(ii) Assume that K is an algebraic extension of F contained in an algebraic closure $\overline{F}$ of F. Then we call K/F a *normal* extension if every embedding of K into $\overline{F}$ that restricts to the identity on F is in fact an automorphism of K. (We say that such an automorphism is an automorphism of K *over* F.)

(iii) A field extension K/F is called a *Galois extension* if it is both separable and normal. The set of all automorphisms of K over F constitutes a group under composition; this is called the *Galois group* of K over F and denoted $\mathrm{Gal}(K/F)$. If $F\subseteq L\subseteq K$ is a tower of fields and K/F is Galois, then K/L is likewise Galois.

Note that these notions do not require that K/F be finite. Our aim now is to extend the fundamental theorem of Galois theory to infinite extensions. This will require the introduction of some topology.

If S is any set of automorphisms of a field F, as usual F^S denotes the fixed field of S in F; that is, the subfield of F consisting of all elements of F left fixed by every automorphism of S.

Suppose that K/F is a Galois extension with Galois group G. Consider the set $\mathcal{N}$ of normal subgroups of G of finite index. If $N, M\in\mathcal{N}$ and $M\subseteq N$, we have a projection map $\rho_{N,M}: G/M \to G/N$, and hence a projective system of quotients $\{G/N\}_{N\in\mathcal{N}}$. This system is certainly compatible with the family of canonical projections $\rho_N : G \to G/N$, which corresponds to the restriction map from $\mathrm{Gal}(K/F)$ to $\mathrm{Gal}(K^N/F)$. Thus we have a canonically induced homomorphism ρ from G into the projective limit of the associated quotients.

1-19 PROPOSITION. *Let K, F, G, and $\mathcal{N}$ be as above. Then the canonical map*

$$\rho : G \to \varprojlim_{N\in\mathcal{N}} G/N$$

is in fact an isomorphism of groups. Hence G is a profinite group in the topology induced by ρ.

In this context, we shall simply speak of the Galois group G as having the profinite topology.

PROOF. We show first that ρ is injective. Certainly

$$\operatorname{Ker}(\rho) = \bigcap_{N \in \mathcal{N}} N$$

and so we need only demonstrate that this intersection is trivial. Let $\sigma \in \operatorname{Ker}(\rho)$ and let $x \in K$. Then by elementary field theory there exists a finite Galois extension F'/F such that $F' \subseteq K$ and $x \in F'$. Now the restriction map from $G = \operatorname{Gal}(K/F)$ to $\operatorname{Gal}(F'/F)$ has kernel $\operatorname{Gal}(K/F')$, which is therefore a normal subgroup of G of finite index. But then $\sigma \in \operatorname{Gal}(K/F')$, and so $\sigma(x) = x$. Since x is arbitrary, σ is the identity on K, and $\operatorname{Ker}(\rho)$ is trivial, as required.

We show next that ρ is also surjective. Fix (σ_N) in the projective limit. Given an arbitrary element $x \in K$, again we know that x lies in some finite Galois extension F' of F with $N = \operatorname{Gal}(K/F')$ normal and of finite index in G and $\operatorname{Gal}(F'/F) = G/N$. Now define $\sigma \in \operatorname{Gal}(K/F')$ by $\sigma(x) = \sigma_N(x)$. By construction of the projective limit, σ is independent of the choice of extension F', and hence is a well defined automorphism of K. Moreover, it is clear that σ_N is $\rho_N(\sigma)$ for all N. ❑

Note that the isomorphism constructed in the previous proposition is essentially field-theoretic, and not merely group-theoretic. (See Exercise 12 below.)

1-20 THEOREM. (The Fundamental Theorem of Galois Theory) *Let K/F be a Galois extension (not necessarily finite) and let $G = \operatorname{Gal}(K/F)$ with the profinite topology. Then the maps*

$$\alpha : L \mapsto H = \operatorname{Gal}(K/L)$$
$$\beta : H \mapsto L = K^H$$

constitute a mutually inverse pair of order-reversing bijections between the set of intermediate fields L lying between K and F, and the set of closed subgroups of G. Moreover, L is Galois over F if and only if the corresponding subgroup H is normal in G.

PROOF. Note that in the case of a finite extension K/F, we may ignore the topological restriction, and the statement amounts to the fundamental theorem of Galois theory for finite extensions, a result that we assume. We proceed in four steps.

STEP 1. We must show first that the map α is well-defined; that is, that α indeed yields closed subgroups of G. (The map β is of course well-defined on ar-

bitrary subsets of G.) According to the previous proposition, H is profinite as the Galois group of K/L, and Exercise 14 shows that this topology is identical to that induced by G. Thus H is a profinite subgroup of a profinite group and is therefore closed by Theorem 1-18.

STEP 2. We claim that $\beta\circ\alpha$ is the identity map. Let L be an intermediate field. By definition $\alpha(L)$ fixes L, and so clearly $\beta(\alpha(L))\supseteq L$. Conversely, suppose that z lies in $\beta(\alpha(L))$. Then since z lies in K and is therefore separable over L, z also belongs to a finite Galois extension M of L contained in K. Let $\bar{\sigma}\in\mathrm{Gal}(M/L)$. Then there exists $\sigma\in\mathrm{Gal}(K/L)$ that restricts to $\bar{\sigma}$. (The extensibility of automorphisms for infinite extensions follows from the finite case by Zorn's lemma.) By construction, $\sigma(z)=z$, and hence $\bar{\sigma}(z)=z$ for all $\bar{\sigma}\in\mathrm{Gal}(M/L)$. But by the fundamental theorem for finite extensions, we know that $z\in L$. Hence we have also that $\beta(\alpha(L))\subseteq L$, and the claim is established.

STEP 3. We shall show now that $\alpha\circ\beta$ is likewise the identity. By definition, for any subgroup H of G we have that $\alpha(\beta(H))\supseteq H$. Now assume that H is closed. Then again by Theorem 1-18, H is the intersection of a family $\mathscr{U}$ of open subgroups of G. Since α and β are clearly order reversing,

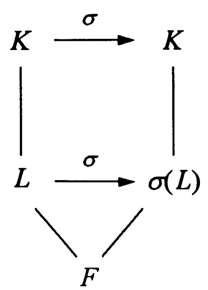
$$\beta(H)=\beta\Big(\bigcap_{U\in\mathscr{U}}U\Big)\supseteq\bigcup_{U\in\mathscr{U}}\beta(U)$$

and

$$\alpha(\beta(H))\subseteq\alpha\Big(\bigcup_{U\in\mathscr{U}}\beta(U)\Big)\subseteq\bigcap_{U\in\mathscr{U}}\alpha(\beta(U))=\bigcap_{U\in\mathscr{U}}U=H\ .$$

The point is that each of the open subgroups U has finite index, and thus in each case $\alpha(\beta(U))=U$ by the finite theory.

STEP 4. Finally, suppose that $\alpha(L)=\mathrm{Gal}(K/L)=H$, where L is some intermediate field. Let σ lie in G. Then from the diagram



we deduce that $\mathrm{Gal}(K/\sigma(L))=\sigma H\sigma^{-1}$. Thus according to parts (i)–(iii) above, we have that $\sigma(L)=L$ for all $\sigma\in G$ if and only if $\sigma H\sigma^{-1}=H$ for all $\sigma\in G$. This is to say that L is normal (and hence Galois) over F if and only if H is normal in G.❑

REMARK. We leave it to the reader to determine the effect of $\alpha\circ\beta$ on an arbitrary subgroup of $\mathrm{Gal}(K/F)$. (See Exercise 15 below.)

1.4 Pro-p-Groups

Our aim here is to introduce for profinite groups an analogue of the p-Sylow subgroups that play such a crucial role in finite group theory. To begin, we must first generalize the notion of order.

Orders of Profinite Groups

DEFINITION. A *supernatural number* is a formal product

$$\prod_p p^{n_p}$$

where p runs over the set of rational primes and each $n_p\in\mathbf{N}\cup\{\infty\}$.

Clearly the set of supernatural numbers is a commutative monoid with respect to the obvious product. If a is a supernatural number, we set $v_p(a)$ equal to the exponent of p occurring in a. We say that *a divides b*, and as usual write $a|b$, if $v_p(a)\leq v_p(b)$ for all primes p. Note that if $a|b$, there exists a supernatural number c such that $ac=b$.

Given supernatural numbers a and b, we may define both their *least common multiple* and *greatest common divisor* by the formulas

$$\mathrm{lcm}(a,b)=\prod p^{\sup(v_p(a),v_p(b))} \quad\text{and}\quad \gcd(a,b)=\prod p^{\inf(v_p(a),v_p(b))} .$$

One extends these notions to arbitrary (even) infinite families of supernatural numbers in the obvious way.

Now let G be a profinite group. As previously, let $\mathcal{N}$ denote the set of all open, normal subgroups of G. Recall that each quotient group G/N, for $N\in\mathcal{N}$, is finite.

DEFINITION. Let H be a closed subgroup of G. Then we define $[G:H]$, the *index of H in G*, by the formula

$$[G:H] = \operatorname*{lcm}_{N \in \mathcal{N}} [G/N:HN/N] \ .$$

In particular, $[G:\{e\}]$, the index of the trivial subgroup, is called the *order* of G and denoted $|G|$.

Using the standard isomorphism between HN/N and $H/H\cap N$, we may recast the definition above as

$$[G:H] = \operatorname*{lcm}_{N \in \mathcal{N}} [G/N:H/H \cap N] .$$

See also Exercise 16 below.

1-21 PROPOSITION. *Let G be a profinite group with closed subgroups H and K such that $H \subseteq K$. Then $[G:K]=[G:H][H:K]$.*

PROOF. Note that since H is closed, it is also profinite, and so the assertion is well defined. Now let N be any open normal subgroup of G. Then

$$[G/N:K/K\cap N] = [G/N:H/H\cap N]\ [H/H\cap N:K/K\cap N] \ . \tag{1.3}$$

The lcm (over $N \in \mathcal{N}$) of either side of the equation is, of course, $[G:H]$. Consider the factors on the right: if we replace N by any smaller subgroup $N_1 \in \mathcal{N}$, both indices are inflated (cf. Exercise 17). Hence, taking intersections, any pair of prime powers occurring in $[G/N:H/H\cap N]$ and $[H/H\cap N:K/K\cap N]$, respectively, may be assumed to occur simultaneously. The upshot is that we can compute the lcm of the product by separately computing the lcm's of each factor. The first yields $[G:H]$; it remains only to show that the second yields $[H:K]$.

Let M be any open, normal subgroup of H. Then $M=H\cap U$, where U is open in G. But by Lemma 1-17, U contains an open, normal subgroup N of G, and one argues as above that

$$[H/M:K/K\cap M] \mid [H/H\cap N:K/K\cap N] \ .$$

Thus $[H:K]$ may be computed as the lcm over subgroups of H of the form $H\cap N$, where N is open and normal in G. Hence the second factor on the right of Eq. 1.3 indeed yields $[H:K]$, as required. ❑

REMARK. The proof shows that we may compute a profinite index as the lcm over any *cofinal* family $\mathcal{M} \subseteq \mathcal{N}$ of open normal subgroups of the ambient group; that is, if for every $N \in \mathcal{N}$ there exists an $M \in \mathcal{M}$ such that $M \subseteq N$, then

$$\operatorname*{lcm}_{N \in \mathcal{N}} [G/N:HN/N] = \operatorname*{lcm}_{M \in \mathcal{M}} [G/M:HM/M] \ .$$

EXAMPLES

(1) Consider the p-adic integers

$$\mathbf{Z}_p = \varprojlim_{n\geq 1}(\mathbf{Z}/p^n\mathbf{Z}) \ .$$

Let H_n denote the kernel of the projection map from $\mathbf{Z}_p$ to $\mathbf{Z}/p^n\mathbf{Z}$. Since this projection is surjective, we have $\mathbf{Z}_p/H_n \cong \mathbf{Z}/p^n\mathbf{Z}$, and it follows that p^∞ divides $|\mathbf{Z}_p|$. Conversely, every finite quotient of $\mathbf{Z}_p$ has order a power of p, and therefore $|\mathbf{Z}_p| = p^\infty$.

(2) Next consider

$$\hat{\mathbf{Z}} = \varprojlim_{n\geq 1}(\mathbf{Z}/n\mathbf{Z}) \ .$$

Arguing as above, every factor group $\mathbf{Z}/n\mathbf{Z}$ occurs as a quotient of $\hat{\mathbf{Z}}$, whence every positive integer is a divisor of its order. Thus

$$|\hat{\mathbf{Z}}| = \prod_{p \text{ prime}} p^\infty \ .$$

Pro-p-Groups

Let p be a rational prime. Recall that a group is called a *p-group* if the order of every element is finite and a power of p. In the case that G is finite, this is equivalent to the statement that the order of G is a power of p.

DEFINITION. A projective limit of finite p-groups is called a *pro-p-group*.

Of course, $\mathbf{Z}_p$ is a pro-p-group; so is $\hat{H}_p$, the projective limit of the Heisenberg groups $H(\mathbf{Z}/p^n\mathbf{Z})$. (See Exercise 18 below.)

1-22 PROPOSITION. *A profinite group G is a pro-p-group if and only if its order is a power of p (possibly infinite).*

PROOF. $\Leftarrow$) We have already seen in the proof of Theorem 1-14 that G is the projective limit of its finite quotient groups G/N. If the order of G is a power of p, then each of these quotients must be a p-group, as required.

$\Rightarrow$) Suppose that G is the projective limit of the projective system P_i of p-groups. Then by definition of the topology of G, cofinal among the open normal subgroups of G are subgroups of the form

$$M = (\prod Q_i) \cap G$$

where $Q_i = P_i$ for all but finitely many indices, and $Q_i = \{e_i\}$ for the exceptions. Now given an arbitrary $x \in G$ and specifying any finite subset of its coordinates, there is clearly a finite exponent of the form $q = p^r$ such that x^q is trivial at each of the specified coordinates. Hence G/M is a p-group, and it follows by the remark following Proposition 1-21 that the order of G is a power of p. ❑

DEFINITION. Let G be a profinite group. A maximal pro-p-subgroup of G is called a *pro-p-Sylow subgroup* of G (or more simply, a *p-Sylow* subgroup of G).

Note that the trivial subgroup may well be a pro-p-subgroup of G for some primes p. The following theorem shows among other things that this is the case if and only if p does not divide the order of G.

1-23 THEOREM. *Let G be a profinite group and let p be a rational prime. Then the following assertions hold:*

(i) *p-Sylow subgroups of G exist.*

(ii) *Any pair of conjugate p-Sylow subgroups of G are conjugate.*

(iii) *If P is a p-Sylow subgroup of G, then $[G:P]$ is prime to p.*

(iv) *Each p-Sylow subgroup of G is nontrivial if and only if p divides the order of G.*

PROOF. As usual, let $\mathscr{N}$ denote the set of open normal subgroups of G and recall the explicit isomorphism

$$\varphi : G \to \varprojlim G/N$$
$$x \mapsto (xN)_{N \in \mathscr{N}} \ .$$

Note in particular that if $x,y \in G$ and $xN = yN$ for every open normal subgroup N, then $x = y$. A similar statement holds for arbitrary subsets of G.

(i) For each $N \in \mathscr{N}$, let $\mathscr{P}(N)$ denote the set of p-Sylow subgroups of the finite group G/N. Then clearly $\mathscr{P}(N)$ is finite and, moreover, nonempty. (If G/N has order prime to p, then the trivial subgroup is a p-Sylow subgroup.) Assume that $M,N \in \mathscr{N}$ with $N \subseteq M$. Then there exists a surjective homomorphism of finite groups $\varphi_{M,N} : G/N \to G/M$. Since this map sends a p-Sylow subgroup of G/N to a p-Sylow subgroup of G/M (refer again to Exercise 17), we obtain an induced map $\varphi_{M,N} : \mathscr{P}(N) \to \mathscr{P}(M)$. Thus we obtain a projective system $(\mathscr{P}(N), \varphi_{M,N})$ of finite nonempty sets, and the projective limit of this system is likewise nonempty by Proposition 1-11. This means that there exists a projective system of

p-Sylow subgroups $(P_N, \varphi_{M,N})$, where for each $N \in \mathcal{N}$, we have $P_N \subseteq G/N$. Let P be the projective limit of the P_N, which we can clearly identify with a subgroup of the projective limit of the G/N and hence with a subgroup of G via φ. Then P is a pro-p-group by construction, and we shall now show that it is maximal. Let Q be any pro-p-subgroup containing P. Then for every open normal subgroup N, $QN/N \supseteq PN/N = P_N$. But Q is a pro-p-group, so by the previous proposition, QN/N is a p-group and therefore equal to the p-Sylow subgroup P_N. Thus for every open normal subgroup N, $QN/N = PN/N$, and therefore Q and P have the same image under φ and accordingly are equal. Hence P is indeed maximal, as claimed.

(ii) Let P and Q be p-Sylow subgroups of G. For every $N \in \mathcal{N}$, we make the following definitions:

$$\begin{aligned} P_N &= PN/N \\ Q_N &= QN/N \\ Y_N &= \{y_N \in G/N : y_N P_N y_N^{-1} = Q_N\} . \end{aligned}$$

Note that each Y_N is finite and, by the Sylow theorems for finite groups, nonempty. Moreover, the subsets Y_N clearly constitute a projective system. Let Y denote the (nonempty) projective limit of the Y_N, which we again identify with a subset of G via φ, and let y lie in Y. Then by construction, yPy^{-1} and Q have equal projection in G/N for all open, normal N and are therefore equal. Hence P and Q are indeed conjugate.

(iii) Let P be a p-Sylow subgroup of G. Then by definition

$$[G:P] = \operatorname*{lcm}_{N \in \mathcal{N}} [G/N : PN/N] .$$

But by Exercise 19, for each N, the subquotient PN/N is a p-Sylow subgroup of G/N, and so by finite group theory each index $[G/N:PN/N]$ is prime to p. Hence $[G:P]$ is likewise prime to p.

(iv) This follows at once from parts (i) and (iii). ❑

1-24 COROLLARY. *Let G be a commutative profinite group. Then the following assertions hold:*

(i) *For every prime p, G admits a unique pro-p-Sylow subgroup.*

(ii) *Let p and q be distinct primes and let P and Q be the corresponding Sylow subgroups. Then $P \cap Q$ is trivial.*

(iii) *G is isomorphic to the direct product of its Sylow subgroups.*

PROOF. (i) In light of the commutativity of G, this follows at once from parts (i) and (ii) of the theorem above.

(ii) The order of $P \cap Q$ must divide powers of both p and q, whence this intersection must be trivial.

(iii) Let N be an open normal subgroup of G. Then for each pro-p-Sylow subgroup P we have a canonical projection from P onto PN/N, the unique p-Sylow subgroup of G/N. Note that this projection is trivial for all but the finitely many primes p that divide the order of G/N. By the theory of finite commutative groups, we have

$$\prod PN/N \cong G/N$$

where the product is taken over all of the Sylow subgroups of G. We may lift this isomorphism to G as follows:

$$\begin{aligned} G &= \varprojlim G/N \\ &= \varprojlim \prod PN/N \\ &= \prod \varprojlim PN/N \\ &= \prod \varprojlim P/P \cap N \\ &= \prod P \ . \end{aligned}$$

All products are over the set of Sylow subgroups of G; all projective limits are over the family of open, normal subgroups of G. The final line of the calculation is justified by the cofinality of subgroups of the form $P \cap N$ among the open subgroups of P, which may be deduced from Lemma 1-17. ❑

EXAMPLE. Recall that the abelian profinite group

$$\hat{\mathbf{Z}} = \varprojlim \mathbf{Z}/n\mathbf{Z}$$

has order $\prod p^\infty$, where the product is taken over all primes. Given a prime p, let P be the unique corresponding p-Sylow subgroup of $\hat{\mathbf{Z}}$. Let P_n denote the unique p-Sylow subgroup of $\mathbf{Z}/n\mathbf{Z}$. Then

$$P = \varprojlim_n P_n = \varprojlim_n \mathbf{Z}/p^{v_p(n)}\mathbf{Z} = \varprojlim_m \mathbf{Z}/p^m\mathbf{Z} = \mathbf{Z}_p \ .$$

Thus according to the corollary, $\hat{\mathbf{Z}} = \prod \mathbf{Z}_p$.

Exercises

1. Let G be a topological group. Show that the topology on G is completely determined by a system of open neighborhoods of the identity e.

2. Let $G=\mathbf{Z}$ and impose the following topology: $U\subseteq G$ is open if either $0\notin U$ or $G-U$ is finite. Show that G is *not* a topological group with respect to this topology. [*Hint*: If so, the mapping $a\mapsto a+1$ would be a homeomorphism; show that it is not.]

3. This exercise shows that we may impose a nondiscrete topology on $\mathbf{Z}$ such that $\mathbf{Z}$ is nonetheless a topological group with respect to addition. Let S^1 denote the multiplicative group of complex numbers of absolute value 1. Recall that an element of $\mathrm{Hom}(\mathbf{Z},S^1)$ is called a *character* of $\mathbf{Z}$. We denote such a character χ. Let

$$\mathscr{G}=\prod_{\chi} S^1$$

where the product is taken over all characters. Then $\mathscr{G}$ is a compact topological group. Now consider the homomorphism

$$\begin{aligned} j:\mathbf{Z}&\to \mathscr{G}\\ n&\mapsto (\chi(n)) \ . \end{aligned}$$

(a) Show that j is injective; that is, show that for any nonzero $n\in\mathbf{Z}$ there exists a character χ such that $\chi(n)\neq 1$.

(b) Let $G=j(\mathbf{Z})$. Then G is a group algebraically isomorphic to $\mathbf{Z}$ and a topological group with respect to the subspace topology induced by $\mathscr{G}$. Show that G is not discrete with respect to this topology and conclude that $\mathbf{Z}$ itself admits a nondiscrete topological group structure with respect to addition. [*Hint*: Suppose that $j(1)$ is open. Then there exists an open subset U of $\mathscr{G}$ such that $U\cap G=j(1)$; moreover, we may assume that all but finitely many projections of U onto its various coordinates yield all of S^1. Noting that $j(1)$ generates the infinite group G, one may now derive a contradiction.]

4. Give an example of a topological group with a closed subgroup that is *not* open.

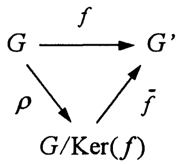
5. Let X be a topological space and let $C(X)$ denote the space of connected components of X. (This constitutes a partition of X). As usual, we impose

the quotient topology on $C(X)$—the strongest topology such that the canonical projection $\rho: X \to C(X)$ is continuous. Show that $C(X)$ is totally disconnected with respect to this topology. [*Hint*: We say that a subset Y of a topological space is *saturated* if whenever $y \in Y$, the entire connected component of y lies in Y. Let F be a connected component of $C(X)$ that contains more than one point. Show that $\rho^{-1}(F)$ is a saturated, closed, disconnected set. Write $\rho^{-1}(F)$ as the disjoint union of two saturated, closed subsets of X, and apply ρ to this decomposition to show that F is in fact disconnected—a contradiction.]

6. Let $G = \mathrm{GL}_n(\mathbf{R})$. Show that G° is the set of $n \times n$ matrices with positive determinant.

7. Let H be a subgroup of the topological group G. Show that its closure $\overline{H}$ is normal (respectively, abelian) if H is.

8. Let $f: G \to G'$ be a surjective continuous homomorphism of topological groups. Show that f factors uniquely through $G/\mathrm{Ker}(f)$; that is, there exists a unique continuous homomorphism $\bar{f}$ such that the following diagram commutes:



Show that $\bar{f}$ is moreover injective. Under what conditions is $\bar{f}$ a topological isomorphism onto its image?

9. Let $f: X \to Y$ be a continuous bijective mapping of topological spaces and assume that X is compact and Y is Hausdorff. Show that f is moreover a homeomorphism. [*Hint*: It suffices to show that f is open. What can one say about the image of U^c under f where U is any open subset of X?]

10. Let I be an index set with preordering defined by equality and let (G_i, φ_{ij}) be a projective system of sets defined with respect to I. What is the projective limit in this case?

11. Give an example of a projective system of finite nonempty sets over a preordered, but not directed, set of indices such that the projective limit is nevertheless itself empty.

12. Let G be an arbitrary group. Show that in general G is not isomorphic to the projective limit of the quotient groups G/N, as N varies over all of the

subgroups of G of finite index. Hence not every abstract group acquires a profinite structure by this device. [*Hint*: Take $G=\mathbf{Z}$.]

13. Let (G_i, φ_{ij}) and (H_i, φ_{ij}) be two projective systems of sets. (Note that we use the same map designators φ_{ij} for both systems.) Suppose that we have a family of maps $\{\zeta_i : G_i \to H_i\}$ that is compatible with these systems in the sense that $\varphi_{ij} \circ \zeta_j = \zeta_i \circ \varphi_{ij}$ for all pairs of indices $i \le j$. Show that there exists a unique map $\zeta: G \to H$ on their respective projective limits such that $\zeta_i \circ p_i = p_i \circ \zeta$ for all i, where p_i denotes the appropriate projection map. Observe that this construction works equally well in the categories of groups, topological spaces, and topological groups. [*Hint*: In light of the universal property of projective limits, consider the family of composed maps $\{\zeta_i \circ p_i : G \to H_i\}$.]

14. Let K/F be a Galois extension with Galois group G.

(a) Let L be an intermediate field that is finite over F. For any given $\sigma \in G$, define $N_L(\sigma) \subseteq G$ to be the set of $\tau \in G$ such that σ and τ agree on L. The subsets $N_L(\sigma)$ constitute a subbase for a topology on G. Show (i) that this topology remains unchanged if we restrict the subbase to normal intermediate fields that are finite over F and (ii) that this topology is identical to the profinite topology on G.

(b) Now let L be an arbitrary intermediate field, and let H denote the Galois group of K over L. Use the characterization of the profinite topology given in part (a) to show that the topology induced on H by G is identical to the profinite topology defined directly on H as Gal(K/L).

15. Let K/F be a Galois extension (not necessarily finite) and let H be any subgroup of $G = \mathrm{Gal}(K/F)$ (not necessarily closed). Let α and β be defined as in Theorem 1-20. Show that $\alpha(\beta(H)) = \overline{H}$, the closure of H.

16. Let G be a profinite group and let H be a closed subgroup. Show that

$$[G:H] = \operatorname*{lcm}_{N \in \mathcal{N}} [G:HN]$$

where $\mathcal{N}$ is the set of all open, normal subgroups of G. Show further that if M is any open subgroup of G containing H, then there exists an open normal subgroup N of G such that $M \supseteq NH$. Conclude from this and the previous equation that moreover,

$$[G:H] = \operatorname*{lcm}_{\substack{M \text{ open} \\ M \supseteq N}} [G:M] \ .$$

17. Let $\varphi: G \to G'$ be a surjective homomorphism of groups with kernel L. Let H be a subgroup of G of finite index and let H' be the image of H under φ. Show that $[G:H]=[G':H']\cdot[HL:H]$.

18. For any commutative ring A with unity, define the *Heisenberg group* $H(A)$ over A by

$$H(A)=\left\{\begin{pmatrix}1 & a & c\\ 0 & 1 & b\\ 0 & 0 & 1\end{pmatrix} : a,b,c\in A\right\} .$$

(a) Show that $H(A)$ is a group under multiplication in the matrix ring $M_3(A)$ and that this construction is, moreover, functorial in A.

To continue, for $n\geq 1$, $H(\mathbf{Z}/p^n\mathbf{Z})$ is clearly a group of order p^{3n}, and hence a p-group. If $m|n$, then by functoriality, we have that the canonical projection $\mathbf{Z}/p^n\mathbf{Z}\to\mathbf{Z}/p^m\mathbf{Z}$ induces a homomorphism φ_{mn} from $H(\mathbf{Z}/p^n\mathbf{Z})$ to $H(\mathbf{Z}/p^m\mathbf{Z})$.

(b) Show that $(H(\mathbf{Z}/p^n\mathbf{Z}),\varphi_{mn})$ is a projective system of groups.

Let $\hat{H}_p$ denote the projective limit of the $H(\mathbf{Z}/p^n\mathbf{Z})$; by definition, this is a pro-p-group.

(c) Show that $H(\mathbf{Z}_p)\cong\hat{H}_p$. [*Hint*: Consider the map

$$\pi_n: H(\mathbf{Z}_p)\to H(\mathbf{Z}/p^n\mathbf{Z})$$

induced by projection from $\mathbf{Z}_p$ onto $\mathbf{Z}/p^n\mathbf{Z}$. Show that this is a continuous surjective homomorphism and that moreover, the family $\{\pi_n\}$ is compatible with the system of homomorphisms $\{\varphi_{mn}\}$. Finally, show that the map π obtained from the π_n by the universal property of the direct limit is the desired isomorphism.]

19. Let G be a profinite group and p a rational prime. For each open, normal subgroup N in G, let H_N be a p-subgroup of G/N (not necessarily a p-Sylow subgroup). Show that there exists a pro-p-Sylow subgroup P of G such that $PN/N\supseteq H_N$ for all N. Conclude (i) that every pro-p-subgroup of G is contained in a pro-p-Sylow subgroup of G; and (ii) that if P is a pro-p-Sylow subgroup of G, then PN/N is a p-Sylow subgroup of G/N for each open, normal subgroup N of G. [*Hint*: Generalize the argument from the proof of part (i) of Theorem 1-23.]

2
Some Representation Theory

The general background for Tate's thesis involves locally compact groups, their representations, and duality theory. Many of these basic prerequisites are derived in this and the next chapter.

Here we develop elements of representation theory for a locally compact topological group G represented in the automorphism group of a topological vector space V. A representation in this context is in fact a restricted instance of an ordinary abstract group representation, with the extra constraints involving continuity and some specific topological conditions on V. Our development is somewhat general without becoming excessively technical; in particular, we postpone the assumption that G is commutative until as late as possible. This is not empty abstraction: the noncommutative case is interesting in its own right, as shown by Jacquet-Langlands theory, which deals with representations of the general linear group.

The key results of this chapter are Schur's lemma for irreducible unitary representations of a topological group G and the theorem that such representations are one-dimensional in the case that G is abelian. Considering that the finite-dimensional analogues of these statements are not particularly deep, they are surprisingly challenging to prove. In fact, the chase will lead us through the spectral theory of Banach algebras, the Gelfand transform, and the spectral theorems. (We state the second spectral theorem for completeness, but make no essential use of it.) The Gelfand transform is especially noteworthy because it is applied again in the following chapter in a wholly different context.

2.1 Representations of Locally Compact Groups

A field k (subject to some given topology) is called a *topological field* if both addition and multiplication are continuous functions on $k \times k$. A vector space V (again subject to some given topology) over k is called a *topological vector space* if the following two conditions are satisfied:

(i) The underlying additive group $\langle V,+\rangle$ is moreover a topological group.

(ii) The scalar multiplication map

$$k \times V \to V$$
$$(\lambda, v) \mapsto \lambda v$$

is continuous (with respect to the product topology on $k \times V$).

EXAMPLES

(1) If k is a topological field and V is any merely algebraic vector space over k, then we have an isomorphism of vector spaces

$$V \cong \prod_I k$$

where I is some index set. We may use the isomorphism to transfer the product topology of $\prod k$ to V. One checks easily that with respect to this induced topology, V is a topological vector space over k. Moreover, for finite-dimensional V, every linear map is clearly continuous, and hence the transferred topology is independent of the choice of isomorphism.

(2) Recall that a normed vector space V over **R** (respectively, over **C**) that is complete with respect to the norm metric is called a real (respectively, complex) *Banach space*. One checks easily that V is a topological vector space over **R** (respectively, **C**) with respect to the norm topology. (Note that any normed space may be embedded in its completion, with the given norm extended by continuity; the completion is *ipso facto* a Banach space.)

Henceforth we shall assume that our topological vector spaces are T_1 (and hence Hausdorff, by Proposition 1-3). This is equivalent to the assertion that $\{0\}$ is a closed subset.

For a topological vector space V over k, we distinguish Aut(V), the group of vector space automorphisms $V \to V$, from $\text{Aut}_{\text{top}}(V)$, the group of topological automorphisms $V \to V$ (i.e., continuous vector space automorphisms with continuous inverse).

Recall that a subset S of a real or complex vector space is called *convex* if for every $x, y \in S$, each point of the form $tx+(1-t)y$, $0 \le t \le 1$, also lies in S. A real or complex topological space is called *locally convex* if there is a base for the topology consisting of convex sets. Thus, for example, the topological vector spaces $\mathbf{R}^n$ and $\mathbf{C}^n$ are both locally convex.

DEFINITION. Let G be a locally compact topological group and let V be a locally convex topological vector space over **C**. Then an *abstract representation of* G is merely a homomorphism $\rho: G \to \text{Aut}(V)$. We call ρ a *topological representation* (or simply a *representation*, without qualifier) if it satisfies the additional condition that the map

$$\begin{aligned} G \times V &\to V \\ (g,x) &\mapsto \rho_g(x) \end{aligned}$$

is continuous with respect to the product topology on $G \times V$. [Note that for $g \in G$ we usually write ρ_g for $\rho(g)$.]

It follows at once from the definition that for a topological representation ρ, the image of G under ρ in fact lies in $\mathrm{Aut}_{\mathrm{top}}(V)$.

2-1 PROPOSITION. *An abstract representation $\rho: G \to \mathrm{Aut}(V)$ is moreover a topological representation of G if and only if it satisfies the following two conditions:*

(i) *For every compact subset K of G, the collection of functions $\rho(K)$ is equicontinuous on V.*

(ii) *For every $x \in V$, the map $g \mapsto \rho_g(x)$ is continuous from G to V.*

PROOF. $\Rightarrow$) Certainly a topological representation satisfies (ii), so we need only argue for (i). Let U be a neighborhood of 0 in V. By continuity, for each $g \in G$, there exists a neighborhood H_g of g in G and a neighborhood W_g of 0 in V such that $\rho_h(x) \in U$ for all $h \in H_g$ and $x \in W_g$. Since K is compact, there is a finite subcollection $H_1, \ldots, H_n$ of the H_g that cover K. Let $W_1, \ldots, W_n$ be the corresponding neighborhoods of 0 in V, and set

$$W = \bigcap_{j=1}^{n} W_j \ .$$

Then for all $g \in K$ and $x \in W$, by construction $\rho_g(x) \in U$, and therefore the collection $\rho(K)$ is equicontinuous, as claimed.

$\Leftarrow$) Let (g,x) lie in $G \times V$. Since V is locally convex, it suffices to show that for any convex neighborhood U of 0 in V, there exist neighborhoods H of g in G and W of 0 in V such that for all $h \in H$, $\rho_h(x+W) \subseteq \rho_g(x) + U$.

Assume that $K \subseteq G$ is a compact neighborhood of g. By condition (i), there exists a neighborhood W of 0 in V such that $\rho_h(w) \in U/2$ for all $h \in K$ and $w \in W$. By condition (ii), there exists a neighborhood H of g contained in K such that for all $h \in H$, likewise $\rho_h(x) - \rho_g(x) \in U/2$. Now for arbitrary $h \in G$ and $w \in V$, we have that

$$\rho_h(x+w) - \rho_g(x) = \rho_h(w) + (\rho_h(x) - \rho_g(x)) \ .$$

Thus, in particular, if $h \in H$ and $w \in W$, then by construction the indicated difference lies in $U/2+U/2$. But of course $U/2+U/2=U$, because U is convex, and this completes the proof. ❑

Note that the set of all mapping from $V \to V$ is the direct product of topological spaces

$$\prod_V V$$

and thus acquires the product topology, which in this case amounts to the topology of pointwise convergence. The subset Aut(V) in turn acquires the subspace topology, and viewed thus, condition (ii) above implies that the representation $\rho: G \to \text{Aut}(V)$ is a continuous mapping. Therefore, given any compact subspace K of G, $\rho(K)$ is compact. Consequently, if V is a Banach space, the Banach-Steinhaus theorem implies that $\rho(K)$ is equicontinuous. Thus we have proved the following corollary:

2-2 COROLLARY. *Suppose that V is a Banach space. Then an abstract representation $\rho: G \to \text{Aut}(V)$ is moreover a topological representation if and only if for every $x \in V$, the map $g \mapsto \rho_g(x)$ is continuous from G to V.* ❑

REMARK. The corollary holds more generally if V is a *barreled space*. See Bourbaki, *Topological Vector Spaces*, Chapter III, §4.2.

Let $\rho: G \to V$ be an abstract representation of G. A subspace W of V is called *$\rho(G)$-invariant* (or simply *G-invariant*, when ρ is understood from the context) if $\rho_g(W) \subseteq W$ for all $g \in G$. Equivalently, if we view V as a module over the group algebra $\mathbf{C}[G]$, then a $\rho(G)$-invariant subspace is exactly a $\mathbf{C}[G]$-submodule. Both the trivial subspace $\{0\}$ and V itself are $\rho(G)$-invariant. The class of representations for which these are the only such invariant subspaces is especially noteworthy.

DEFINITION. An abstract representation (ρ, V) is called *algebraically irreducible* if it admits no proper, nontrivial $\rho(G)$-invariant subspaces. A topological representation (ρ, V) is called *topologically irreducible* (or simply *irreducible*, without qualifier) if it admits no closed, proper, nontrivial $\rho(G)$-invariant subspaces.

Algebraic irreducibility of course implies topological irreducibility, but not conversely.

Given a representation (ρ, V) of G, we can vary ρ by any homeomorphic change of basis to obtain another representation that is essentially the same

object. We generalize this notion of equivalence just slightly in the following definition to accommodate the possibility of distinct representation spaces:

DEFINITION. We call two representations (ρ, V) and (ρ', V') *equivalent* and write $(\rho, V)\cong(\rho', V')$ if there exists a topological isomorphism $T: V\to V'$ such that

$$T \circ \rho_g = \rho'_g \circ T \tag{2.1}$$

for all $g\in G$; that is, for all $g\in G$, the following diagram commutes:

$$\begin{array}{ccc} V & \xrightarrow{T} & V' \\ \rho_g \downarrow & & \downarrow \rho'_g \\ V & \xrightarrow[T]{} & V' \end{array}$$

One checks easily that Eq. 2.1 amounts to the assertion that T is a topological isomorphism of $\mathbf{C}[G]$-modules. Accordingly, we sometimes call T a *G-isomorphism*. (More generally, an arbitrary linear transformation from V to V' that respects the action of G is called *G-linear*.)

2.2 Banach Algebras and the Gelfand Transform

Let A and B be Banach spaces defined over the same field. Recall that a linear transformation T from A to B is called a *bounded operator* if there exists a real constant c such that

$$\|T(a)\| \leq c\|a\| \tag{2.2}$$

for all $a\in A$. It is well known that a linear transformation T is a bounded operator if and only if T is continuous. Henceforth $\mathrm{Hom}(A,B)$ denotes the space of all bounded operators from A to B. If $T\in\mathrm{Hom}(A,B)$, then the smallest c that makes inequality 2.2 true is called the *norm* of T and denoted $\|T\|$. One shows easily that $\mathrm{Hom}(A,B)$ is itself a Banach space with respect to this norm. In the special case $A=B$, we write $\mathrm{End}(A)$ for $\mathrm{Hom}(A,A)$. [Keep in mind that the morphisms in $\mathrm{Hom}(A,B)$ and $\mathrm{End}(A)$ are always topological as well as algebraic.]

Let A be a complex algebra that also admits the structure of a complex Banach space. Then A is called a *Banach algebra* if the norm is also *submultiplicative*; that is, if

$$\|ab\| \leq \|a\|\cdot\|b\| \tag{2.3}$$

for all $a,b\in A$. Throughout, we assume that our Banach algebras are *unital*; this is to say that A contains a multiplicative identity 1_A. As usual, the group of

units of A will be denoted $A^\times$. We can always renorm A without disturbing its topology to arrange that $\|1_A\|=1$, and henceforth we do so. (See Exercises 2 and 3 below.)

If A is a Banach algebra, each $a\in A$ acts on A by left multiplication. Let us denote this map ρ_a. Then according to the inequality 2.3, for all $b\in A$, we have that $\|\rho_a(b)\|=\|ab\|\leq\|a\|\cdot\|b\|$, whence $\|\rho_a\|\leq\|a\|$, the former norm being computed of course in End(A). Since we assume that $\|1_A\|=1$, also $\|a\|=\|\rho_a(1_A)\|\leq\|\rho_a\|$, and thus the norm of a as an element of A agrees with its norm as an element of End(A).

Again let $a\in A$ and assume now that $\|a\|<1$. Then one shows easily that the series $\Sigma_{j=0}^{\infty} a^j$ converges (see Exercise 4 below), whence we observe that $(1-a)$ lies in $A^\times$ with

$$(1-a)^{-1}=\sum_{j=0}^{\infty} a^j \ . \tag{2.4}$$

We shall need this observation for the following result.

2-3 PROPOSITION. *Let A be a Banach algebra as above. Then $A^\times$ is an open subset of A. Moreover, the mapping*

$$\begin{aligned} A^\times &\to A^\times \\ a &\mapsto a^{-1} \end{aligned}$$

is a homeomorphism.

PROOF. Let $a\in A^\times$ and suppose that for $b\in A$ we have that $\|a-b\|<\|a^{-1}\|^{-1}$. Then it follows that $\|a^{-1}(a-b)\|<1$, whence by the preceding observation we find that the difference $1-a^{-1}(a-b)$ lies in $A^\times$. But then also $b=a(1-a^{-1}(a-b))\in A^\times$, showing that $A^\times$ is open. The second statement follows at once, since the map $a\mapsto a^{-1}$ is continuous on $A^\times$ and is its own inverse. ❑

With these preliminaries in hand, we now come to one of the principal definitions of this section, essentially a generalization of the notion of an eigenvalue familiar from linear algebra.

DEFINITION. Let A be a complex Banach algebra and let $a\in A$. Then the *spectrum* of A, denoted sp(a), is the subset of **C** defined as follows:

$$\mathrm{sp}(a)=\{\lambda\in\mathbf{C}:\lambda\cdot 1_A-a\notin A^\times\} \ .$$

We shall see below that the spectrum of an element $a\in A$ is never empty. Hence we may define r(a), the *spectral radius* of a, by

$$\mathrm{r}(a)=\sup\{|\lambda|:\lambda\in\mathrm{sp}(a)\} \ .$$

[For the moment, we can take the spectral radius to be 0 if sp(a) is empty.] The *resolvent set* of a is the complement of sp(a) in $\mathbf{C}$. By construction, if λ lies in the resolvent set, then $(\lambda\cdot 1_A - a)^{-1}$ exists in A.

2-4 PROPOSITION. *Let A be a complex Banach algebra as above, and let $p(x)$ be a polynomial with complex coefficients. Then for all $a\in A$, if $\lambda\in$ sp(a), then $p(\lambda)\in$ sp($p(a)$).*

PROOF. Suppose that $p(x) = \sum_{j=0}^{n} \alpha_j x^j$. Then we may compute that

$$\begin{aligned} p(\lambda)\cdot 1_A - p(a) &= \sum_{j=1}^{n} \alpha_j(\lambda^j \cdot 1_A - a^j) \\ &= (\lambda\cdot 1_A - a)b \end{aligned}$$

where b is some element of the algebra A for which we need no explicit calculation, but only the modest observation that b commutes with a. The point is this: if the left-hand side of the preceding equation has inverse c, then $\lambda\cdot 1_A - a$ has inverse bc, a contradiction, since λ is assumed to lie in the spectrum of a. ❑

REMARK. This result generalizes to convergent power series over $\mathbf{C}$. (See Exercise 5 below.)

2-5 LEMMA. *Let $a\in A$. Then* $\mathrm{r}(a) \le \inf \|a^n\|^{1/n}$.

PROOF. We first show that sp(a) lies in the closed disk around zero of radius $\|a\|$. Note that in general for nonzero λ we have $(\lambda\cdot 1_A - a) = \lambda(1_A - \lambda^{-1}a)$. Thus if $|\lambda| > \|a\|$, Eq. 2.4 applies to show that $(\lambda\cdot 1_A - a)$ is invertible. Now let $\lambda\in$ sp(a). Then by the previous proposition, $\lambda^n\in$ sp(a^n) for all $n\ge 0$, and therefore, by the first part of the argument, $|\lambda|^n \le \|a^n\|$. Taking nth roots yields the stated inequality. ❑

The following theorem is the first major result about the spectrum of an element. The proof requires three substantial, but familiar, results: Liouville's theorem, the Hahn-Banach theorem, and the Cauchy integral formula. Recall that if A is a complex Banach space, then A^*, the *dual space*, denotes the space of all continuous (equivalently, bounded) linear maps from A to $\mathbf{C}$.

2-6 THEOREM. *Let A be a complex unital Banach algebra. Then for every $a\in A$* sp(a) *is nonempty and compact. Moreover, the sequence $\|a^n\|^{1/n}$ converges to the spectral radius of a.*

PROOF. We first show that the spectrum is at least compact. Consider the continuous mapping

$$\begin{aligned}&\mathbf{C}\to A\\&\lambda\mapsto(\lambda\cdot 1_A-a)\ .\end{aligned}$$

The resolvent of a is simply the inverse image of $A^\times$ under this map. But then since $A^\times$ is open, so is the resolvent. Consequently the spectrum of a is closed and, according to the previous result, also bounded. Therefore sp(a) is compact.

We next show that sp(a) is nonempty. Fixing an arbitrary $\varphi\in A^*$, define a complex-valued function f on the resolvent set of a by the formula

$$f(\lambda)=\varphi((\lambda\cdot 1_A-a)^{-1})\ .$$

Note that for μ sufficiently close to zero, we have

$$\begin{aligned}f(\lambda-\mu)&=\varphi([(\lambda-\mu)\cdot 1_A-a]^{-1})\\&=\varphi([(\lambda\cdot 1_A-a)(1_A-\mu(\lambda\cdot 1_A-a)^{-1}]^{-1})\\&=\varphi(\sum_{n=0}^{\infty}\mu^n(\lambda\cdot 1_A-a)^{-n-1})\\&=\sum_{n=0}^{\infty}\mu^n\varphi((\lambda\cdot 1_A-a)^{-n-1})\ .\end{aligned}$$

(The last step follows from the linearity and continuity of f.) Thus f has a valid power series expansion at every point of its domain and is accordingly holomorphic. Moreover, if $|\lambda|>||a||$, we have

$$\begin{aligned}f(\lambda)&=\varphi((\lambda\cdot 1_A-a)^{-1})\\&=\varphi(\lambda^{-1}(1_A-\lambda^{-1}a)^{-1})\\&=\varphi(\sum_{n=0}^{\infty}\lambda^{-n-1}a^n)\\&=\sum_{n=0}^{\infty}\lambda^{-n-1}\varphi(a^n)\end{aligned}\tag{2.5}$$

and we can therefore bound f as follows:

$$\begin{aligned}|f(\lambda)|&\le\sum_{n=0}^{\infty}|\lambda|^{-n-1}||\varphi||\cdot||a||^n\\&=\frac{||\varphi||}{|\lambda|-||a||}\ .\end{aligned}$$

Now assume that the spectrum of a is empty, whence a is nonzero. Then f is entire, bounded on the closed disk $|\lambda| \leq 2\|a\|$ by general principles, and bounded elsewhere by the quotient $\|\varphi\|/\|a\|$ according to the previous inequality. By Liouville's theorem, f must be constant, and since clearly $\lim f(\lambda) \to 0$ as $|\lambda| \to \infty$, this constant must be 0. Since this holds for arbitrary $\varphi \in A^*$, it follows from the Hahn-Banach theorem that $(\lambda \cdot 1_A - a)^{-1}$ is 0, which is impossible. Hence sp(a) is nonempty.

Finally, it remains to establish that the spectral radius of a is as stated, and in establishing this, we may certainly assume that a^n is nonzero for all $n \in \mathbf{N}$. First we claim that the power series expansion for f given in Eq. 2.5, which was established for $|\lambda| > \|a\|$, in fact holds with uniform convergence for $|\lambda| \geq r$, for all r greater than the spectral radius of a. To see this, consider the auxiliary function

$$g(\lambda) = \begin{cases} f(\lambda^{-1}) & \text{for } \lambda \neq 0 \\ 0 & \text{otherwise.} \end{cases}$$

Since as we have seen, f is holomorphic for $|\lambda| \geq r > \mathrm{r}(a)$, the power series representation

$$g(\lambda) = \sum_{n=0}^{\infty} \lambda^{n+1} \varphi(a^n)$$

extends to the entire closed disk $|\lambda| \leq r^{-1}$. Moreover, the Cauchy integral formula tells us that for $|\lambda| \leq r^{-1}$ the remainder g_{n+1} after n terms is given by

$$g_{n+1}(\lambda) = \frac{\lambda^{n+1}}{2\pi i} \int_C \frac{g(\zeta)}{\zeta^{n+1}(\zeta - \lambda)} d\zeta$$

where the integral is taken over the circle C of radius strictly between r^{-1} and $\mathrm{r}(a)^{-1}$. It follows easily from this that this remainder is bounded independently of λ. The upshot is that since g is represented by the uniformly convergent power series given above for $|\lambda| \leq r^{-1}$, f is correspondingly represented by the power series representation of Eq. 2.5 with uniform convergence for $|\lambda| \geq r$, as claimed.

Next let $\lambda = re^{i\theta}$, where $r > \mathrm{r}(a)$. We may then integrate the series for $\lambda^{n+1} f(\lambda)$ with respect to θ as follows:

$$\begin{aligned} \int_0^{2\pi} r^{n+1} e^{i(n+1)\theta} f(re^{i\theta}) d\theta &= \sum_{m=0}^{\infty} \int_0^{2\pi} r^{n-m} e^{i(n-m)\theta} \varphi(a^m) d\theta \\ &= 2\pi \varphi(a^n) \ . \end{aligned}$$

Moreover, this value is clearly bounded by $2\pi r^{n+1}M(r)\|\varphi\|$, where

$$M(r) = \sup_{\theta} \| re^{i\theta} \cdot 1_A - a \| \ .$$

Thus

$$|\varphi(a^n)| \leq r^{n+1} M(r) \| \varphi \|$$

for all $\varphi \in A^*$. Appealing again to the Hahn-Banach theorem, we see that the linear mapping $\gamma a^n \mapsto \gamma \|a^n\|$ ($\gamma \in \mathbf{C}$), which is obviously of norm 1, extends from the one-dimensional subspace spanned by $a^n (\neq 0)$ to an element $\varphi \in A^*$ of lesser or equal norm. In this special case, the previous inequality reduces to

$$\|a^n\| \leq r^{n+1} M(r) \ .$$

Since this holds for all $r > \mathrm{r}(a)$, taking nth roots and limits we find that

$$\limsup \|a^n\|^{1/n} \leq \mathrm{r}(a) \ .$$

This inequality together with Lemma 2-5 shows that the sequence $\|a^n\|^{1/n}$ is indeed convergent to the spectral radius of a. ❑

2-7 COROLLARY. (Gelfand-Mazur) *If A is a division ring, then $A \cong \mathbf{C}$.*

PROOF. Given $a \in A$, there exists $\lambda \in \mathrm{sp}(a)$, so that $\lambda \cdot 1_A - a$ is not invertible. But if A is a division ring, then $\lambda \cdot 1_A - a = 0$, whence every element of A takes the form $\lambda \cdot 1_A$ for some complex λ. Then evidently, $A \cong \mathbf{C}$. ❑

Quotient Algebras

In preparation for the discussion of the Gelfand transform, we make some brief remarks on the quotient of a Banach algebra A by a (two-sided) ideal J, which in particular is a linear subspace of A. Recall that as an algebra, A/J consists of the cosets $a+J$. We say that *a represents* its associated coset, and addition and multiplication of cosets are defined by the addition and multiplication of associated representatives. We define a seminorm on A/J by the formula

$$\|a+J\| = \inf\{\|a-x\| : x \in J\} \ . \tag{2.6}$$

It is easy to see that this is well-defined and lacks being a norm only insofar as it is possible that $\|a+J\| = 0$ without it being the case that a represents the zero element of the quotient.

2-8 PROPOSITION. *Assume that J is closed in A. Then* Eq. 2.6 *defines a norm on A/J, and A/J is likewise a Banach algebra with respect to this norm.*

PROOF. In light of the preceding remarks, it suffices to show that the seminorm on the quotient is submultiplicative and yields zero only on the zero element of the quotient space. We consider first the latter point. If $\|a+J\|=0$, there must exist a sequence of points in J converging to a. But since J is assumed closed, this means that $a\in J$, whence $a+J=J$, as required.

It remains to show that the seminorm on A/J is submultiplicative; that is,

$$\|ab+J\| \le \|a+J\|\cdot\|b+J\| \ .$$

First note that since J is a linear subspace, $\|a+J\|$ can equally well be defined as $\inf\{\|a+x\| : x\in J\}$. Accordingly,

$$\begin{aligned}\|a+J\|\cdot\|b+J\| &= \inf_{x\in J}\|a+x\|\cdot\inf_{y\in J}\|b+y\| \\ &\ge \inf_{x,y\in J}\|ab+xb+ay+xy\| \\ &\ge \inf_{x\in J}\|ab+x\| \\ &= \|ab+J\| \ .\end{aligned}$$

The first inequality in the calculation is justified by the submultiplicative nature of the norm on A; the second is justified because the sum $xb+ay+xy$ clearly lies in the ideal J, provided that x and y do. This completes the proof. ❑

REMARK. Note that if J is an ideal of the Banach algebra A, then in particular, J is a subgroup of a topological group, and we may infer from Proposition 1-1 that the closure of J is likewise a subgroup of A. Moreover, since the norm is submultiplicative, if $\{x_j\}$ is a convergent sequence in J, then so are the sequences $\{ax_j\}$ and $\{x_ja\}$ for all $a\in A$. It follows that the closure of J is likewise an ideal of A.

The Gelfand Transform

In this subsection we specialize to commutative complex Banach algebras (always assumed to be unital). If A is such an algebra, a *character* of A is simply a nontrivial (hence surjective and unital) homomorphism of complex algebras from A to $\mathbf{C}$. The set of all characters of A is denoted $\hat{A}$.

2-9 PROPOSITION. *Let A be as above. Then the following statements hold:*

(i) *Every maximal ideal of A is closed.*

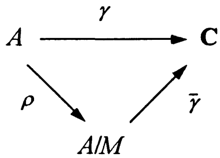
(ii) *The mapping* $\gamma \mapsto \operatorname{Ker}\gamma$ *constitutes a bijective correspondence between* $\hat{A}$ *and the set of maximal ideals of* A.

(iii) *Every element of* $\hat{A}$ *is continuous*

(iv) *For every* $a \in A$, $\operatorname{sp}(a) = \{\gamma(a) : \gamma \in \hat{A}\}$.

PROOF. (i) Let M be a (two-sided) maximal ideal of A; that is, M is a proper ideal of A and there exist no ideals properly between M and A. By the remark above, $\overline{M}$, the closure of M, is likewise an ideal of A, and so to show that $\overline{M} = M$ it suffices to show that $\overline{M}$ is a proper ideal; that is, that $\overline{M}$ excludes all units. But since $A^{\times}$ is open by Proposition 2-3, any unit in $\overline{M}$ must be the limit of units already included in M, contradicting the assumption that $M \neq A$. Hence the maximal ideal M is closed, as claimed.

(ii) Since every character γ is surjective, the quotient $A/\operatorname{Ker}\gamma$ is a field. Hence $\operatorname{Ker}\gamma$ is maximal, and the given mapping is at least well-defined. Let M be the closed ideal $\operatorname{Ker}\gamma$. Then we have the following commutative diagram:



Here ρ denotes the canonical projection onto the quotient (a continuous homomorphism of Banach algebras), and $\bar{\gamma}$ is the unique induced map on the quotient, which is at least an isomorphism of complex algebras. Every element of A/M takes the form $z \cdot 1_A + M$ for some $z \in \mathbf{C}$, and in fact the induced isomorphism is precisely

$$\bar{\gamma}(z \cdot 1_A + M) = z \ .$$

Note that $\bar{\gamma}$ is, moreover, continuous: for open $U \subseteq \mathbf{C}$,

$$\bar{\gamma}^{-1}(U) = U \cdot 1_A + M = \rho(U \cdot 1_A)$$

which is evidently open in A/M.

Conversely, if M is any maximal ideal of A, then A/M is not only a Banach algebra but also a field, which by Corollary 2-7 is isomorphic to $\mathbf{C}$. Call this isomorphism $\bar{\gamma}_M$. Then the diagram above defines a character $\gamma_M = \bar{\gamma}_M \circ \rho$, and it is straightforward to check that for all characters γ,

$$\gamma_{\operatorname{Ker}\gamma} = \gamma$$

and for all maximal ideals M,

$$\operatorname{Ker} \gamma_M = M \ .$$

This establishes the claim.

(iii) The continuity of an arbitrary character γ follows at once from its factorization above into two continuous maps.

(iv) Let $a \in A$. Then $\lambda \in \mathrm{sp}(a)$ if and only if $(\lambda \cdot 1_A - a)$ is not a unit of A, and hence (by Zorn's Lemma) if and only if $(\lambda \cdot 1_A - a)$ is contained in some maximal ideal M. But by part (ii) this occurs if and only if $(\lambda \cdot 1_A - a)$ lies in the kernel of some character γ, which is to say, if and only if $\gamma(a) = \lambda$ for some γ. ❑

We next introduce a topology on $\hat{A}$, the space of characters on A, by duality. As a preliminary, note that for each $a \in A$, we have an associated map from A^* to **C** defined by $\varphi \mapsto \varphi(a)$; this is simply evaluation at a. Recall that one then defines the *weak-star* topology on A^* (abbreviated to the w^*- topology on A^*) to be the weakest topology on A with respect to which all such evaluation maps are continuous. Under this topology A^* is a locally convex topological vector space and, in particular, Hausdorff. (See Appendix A; especially sections A.2 and A.3.) Moreover, convergence in the w^*-topology amounts precisely to pointwise convergence.

Part (iii) of the previous result shows that in fact $\hat{A}$ lies in A^*. The subspace topology on $\hat{A}$ induced by the w^*-topology on A^* is called the *Gelfand topology* on $\hat{A}$.

2-10 LEMMA. *The space $\hat{A}$ of characters on A lies in the unit ball of the dual space A^*. Moreover, $\hat{A}$ is both Hausdorff and compact with respect to the Gelfand topology.*

PROOF. For each $a \in A$ and $\gamma \in \hat{A}$, we see from Proposition 2-5 and Proposition 2-9, part (iv), that

$$\gamma(a) \leq \mathrm{r}(a) \leq \|a\| \ . \tag{2.7}$$

Thus $\|\gamma\| \leq 1$, and $\hat{A}$ lies in the unit ball of the dual space A^*, as claimed.

The Gelfand topology on $\hat{A}$ is clearly Hausdorff, since it is induced from a Hausdorff topology on A^*. Since the unit ball in A^* is compact by Alaoglu's theorem, to show that $\hat{A}$ is compact, it suffices to show that it is closed. But if γ is the limit of a convergent net $\{\gamma_\alpha\}$ in $\hat{A}$, then $\gamma(a) = \lim \gamma_\alpha(a)$ for all $a \in A$, so that γ is again a nontrivial homomorphism of complex algebras; that is, $\gamma \in \hat{A}$, and therefore $\hat{A}$ is closed, as required. ❑

For each $a \in A$ and $\gamma \in \hat{A}$, define $\hat{a}(\gamma) = \gamma(a)$. Note that by construction each of the functions $\hat{a}$ from $\hat{A}$ to **C** is continuous with regard to the Gelfand topology.

Let $\mathscr{C}(\hat{A})$ denote the algebra of complex-valued functions on $\hat{A}$ that are continuous with respect to the Gelfand topology, and endow $\mathscr{C}(\hat{A})$ with the sup norm. Then the mapping

$$\begin{aligned}\Gamma: A &\to \mathscr{C}(\hat{A}) \\ a &\mapsto \hat{a}\end{aligned}$$

is called the *Gelfand transform*. The following theorem summarizes its fundamental properties.

2-11 THEOREM. *Let A be a complex, unital, commutative Banach algebra with character space $\hat{A}$. Then the following statements hold:*

(i) *The Gelfand transform $\Gamma: A \to \mathscr{C}(\hat{A})$ is a norm-decreasing homomorphism of unital complex algebras.*

(ii) *The image of Γ separates points in $\hat{A}$.*

(iii) *For every $a \in A$, $\hat{a}(\hat{A}) = \mathrm{sp}(a)$ and $\|\hat{a}\|_\infty = \mathrm{r}(a)$, the spectral radius of a.*

(iv) *The kernel of Γ is the radical of A; that is, the intersection of all maximal ideals of A. Equivalently, the kernel of Γ consists of all element of A having spectral radius* 0.

(v) *Γ is injective if and only if A is semisimple; that is, if and only if the radical of A is trivial.*

PROOF. (i) It is straightforward to verify that Γ is a homomorphism of algebras. For instance,

$$\Gamma(ab)(\gamma) = \gamma(ab) = \gamma(a)\gamma(b) = (\Gamma(a)\Gamma(b))(\gamma) \ .$$

Moreover, Γ is norm-decreasing by Eq. 2.7.

(ii) If γ_1 and γ_2 are distinct characters, then $\gamma_1(a) \neq \gamma_2(a)$ for some $a \in A$. Therefore $\hat{a} \in \hat{A}$ separates γ_1 and γ_2.

(iii) This is the content of Proposition 2-9, part (iv), and the definition of the spectral radius.

(iv) Since every character γ factors through A/M for some maximal ideal M, the only elements $a \in A$ that evaluate to zero under every character γ must lie in the intersection of all maximal ideals of A, as claimed. The second statement follows from the previous part.

(v) This follows at once from (iv), to complete the proof. ❑

2.3 The Spectral Theorems

We begin with the complex extension of a familiar theorem in real analysis. A linear space A of complex-valued functions is called *self-adjoint* if for every $f \in A$, its complex conjugate $\bar{f}$ is also in A. From the identity

$$f = \frac{(f+\bar{f})}{2} + i\frac{(f-\bar{f})}{2i}$$

one sees at once that A is self-adjoint if and only if $A = A_{\mathbf{R}} + iA_{\mathbf{R}}$, where $A_{\mathbf{R}}$ denotes the subspace of real-valued functions in A.

Now let X be a compact Hausdorff space and let $\mathscr{C}(X)$ denote the space of continuous complex-valued functions on X. Assume that A is not only a self-adjoint subspace, but moreover a unital subalgebra of $\mathscr{C}(X)$, so that in particular A contains the constant functions. If A separates points, then so must $A_{\mathbf{R}}$, and the real-variable case of the Stone-Weierstrass theorem applies to prove the following extension:

2-12 PROPOSITION. *Let A be a self-adjoint unital subalgebra of $\mathscr{C}(X)$ that separates points. Then A is uniformly dense in $\mathscr{C}(X)$ with respect to the sup norm.* ❑

This form of the Stone-Weierstrass theorem is critical to the first of our spectral theorems and appears in the proof via the following corollary. To state this corollary, we need to introduce for a locally compact Hausdorff topological space X a class of functions somewhat larger than the class of complex-valued continuous functions on X with compact support. Accordingly, we define $\mathscr{C}_0(X)$ to be the set of continuous functions $f: X \rightarrow \mathbf{C}$ such that for each $\varepsilon > 0$, the set $\{x \in X : |f(x)| \geq \varepsilon\}$ is compact. If $X' = X \cup \{\omega\}$ is the Alexandroff one-point compactification of X, then it is easily verified that $f \in \mathscr{C}_0(X)$ if and only if f extends to a continuous complex-valued function $\tilde{f}$ on $\mathscr{C}(X')$ such that $f(\omega) = 0$.

2-13 COROLLARY. *Let X be a locally compact Hausdorff space and let A be a self-adjoint subalgebra of $\mathscr{C}_0(X)$ that separates points with the additional property that for every $x \in X$ there exists an $f \in A$ such that $f(x) \neq 0$. Then A is uniformly dense in $\mathscr{C}_0(X)$ with respect to the sup norm.*

PROOF. Again let X' denote the one-point compactification of X. (Note that this makes sense even if X is already compact, in which case we have simply adjoined an isolated point.) Identify A with a subalgebra of $\mathscr{C}(X')$ by extending each element to a function that vanishes at ω, and let A' be the subalgebra of $\mathscr{C}(X')$ generated by A and the complex constant functions. Then A' is evidently self-adjoint and unital. Moreover, A' separates points: since A already separates

points in X, we need only observe that by hypothesis, for every $x \in X$ there is a function $f \in A$ that does not vanish at x, while by construction its extension to X' does vanish at ω. The previous result now applies to show that A' is uniformly dense in $\mathscr{C}(X')$. Thus for each $g \in \mathscr{C}_0(X)$ [tacitly identified with an element of $\mathscr{C}(X')$] and for each positive ε there exists an $f \in A$ [again identified with an element of $\mathscr{C}(X')$] and a $\lambda \in \mathbf{C}$ such that

$$|g(x) - f(x) + \lambda| < \varepsilon/2$$

for all $x \in X'$. Since both f and g vanish at ω, it follows that $|\lambda| < \varepsilon/2$, and therefore f and g differ on X by less than ε, as required. ❑

Bounded Operators on Hilbert Spaces

In this subsection we specialize our analysis to the Banach algebra of bounded operators on a Hilbert space. Actually, only a few formal aspects of such an algebra will be needed, and these we highlight below.

First recall that a *positive definite Hermitian form* on a complex vector space H is a mapping

$$\begin{aligned} H \times H &\to \mathbf{C} \\ (v,w) &\mapsto \langle v|w\rangle \end{aligned}$$

that satisfies the following properties:

(i) $\langle u|u\rangle \in \mathbf{R}_+$ $(u \in H)$, with equality if and only if $u = \mathbf{0}$

(ii) $\langle u|v\rangle = \overline{\langle v|u\rangle}$ $(u,v \in H)$

(iii) $\langle \lambda u + \mu v|w\rangle = \lambda\langle u|w\rangle + \mu\langle v|w\rangle$ $(u,v,w \in H;\ \lambda,\mu \in \mathbf{C})$

Note that (ii) and (iii) imply also:

(iii)′ $\langle u|\lambda v + \mu w\rangle = \bar{\lambda}\langle u|v\rangle + \bar{\mu}\langle u|w\rangle$ $(u,v,w \in H;\ \lambda,\mu \in \mathbf{C})$

That is, the form $\langle\,|\,\rangle$ is positive definite, conjugate symmetric, linear in the first variable, and conjugate linear in the second.

A complex vector space H together with a positive definite Hermitian form is called a *pre-Hilbert space*. One shows easily that $\langle\,|\,\rangle$ defines a norm on H as follows:

$$\|v\| = \sqrt{\langle v|v\rangle}\ .$$

If H is moreover complete with respect to the associated metric, then H is called a *Hilbert space*. In particular, H is a complex Banach space, and therefore a topological vector space with respect to the topology induced by the norm.

Assume for the remainder of this discussion that H is a Hilbert space, and in accordance with previous usage let End(H) denote the space of bounded linear maps from H to itself. End(H) is thus a Banach algebra with respect to addition and composition of functions, and it acquires some significant new structure from H. In particular, it is well known (see Exercises 9 and 10 below) that for every $T \in \mathrm{End}(H)$ there exists a unique element $T^* \in \mathrm{End}(H)$, called the *adjoint* of T, such that

$$\langle Tx | y \rangle = \langle x | T^* y \rangle$$

for all $x, y \in H$. Moreover, the adjoint has the following elementary properties:

(i) For all $T \in \mathrm{End}(H)$, $T^{**} = T$; that is, the adjoint operator has period two.

(ii) For all $T_1, T_2 \in \mathrm{End}(H)$ and $\lambda_1, \lambda_2 \in \mathbf{C}$, $(\lambda_1 T_1 + \lambda_2 T_2)^* = \overline{\lambda}_1 T_1^* + \overline{\lambda}_2 T_2^*$; that is, the adjoint operator is conjugate linear.

(iii) For all $T_1, T_2 \in \mathrm{End}(H)$, $(T_1 T_2)^* = T_2^* T_1^*$; that is, the adjoint operator is antimultiplicative.

(iv) For all $T \in \mathrm{End}(H)$, $\|T\| = \|T^*\|$; that is, the adjoint operator is an isometry; in particular, the adjoint operator is continuous.

(v) For all $T \in \mathrm{End}(H)$, $\|T T^*\| = \|T\|^2$.

The usual arguments from linear algebra suffice to establish properties (i)–(iii). To establish (iv) and (v), note that for all T,

$$\|T(x)\|^2 = \langle T(x) | T(x) \rangle = \langle T^*T(x) | x \rangle \le \|T^*T\| \cdot \|x\|^2 \ .$$

This shows that $\|T\|^2 \le \|T^*T\|$. But also $\|T^*T\| \le \|T\| \cdot \|T^*\|$, so we have the chain of inequalities

$$\|T\|^2 \le \|T^*T\| \le \|T^*\| \cdot \|T\|$$

and it follows that $\|T\| \le \|T^*\|$ for all T. By symmetry, we deduce that $\|T\| = \|T^*\|$, thus proving (iv). In light of the previously displayed chain, property (v) is now immediate.

The following terminology, largely familiar from linear algebra, is most useful: An element $T \in \mathrm{End}(H)$ is called *normal* if T commutes with T^*; that is, if $T^*T = TT^*$. An endomorphism T is called *self-adjoint* or *Hermitian* if it is equal to its adjoint; that is, if $T^* = T$. The endomorphism T is called *unitary* if its adjoint is equal to its inverse; that is, if $T^{-1} = T^*$. Both self-adjoint and unitary operators are automatically normal.

It follows at once from property (v) above that if $T \in \mathrm{End}(H)$ is self-adjoint, then $\|T^2\| = \|T\|^2$, whence

$$\|T^{2^n}\| = \|T\|^{2^n} \tag{2.8}$$

for all $n \geq 0$.

REMARK. Let A be a complex algebra. An operator $a \mapsto a^*$ on A is called an *involution* if (a) the operator $*$ has period two; (b) the operator $*$ is conjugate linear; (c) the operator $*$ is antimultiplicative. If A is further a Banach algebra and (d) the operator $*$ moreover satisfies the identity $\|aa^*\| = \|a\|^2$ for all $a \in A$, we call A a *C^*-algebra.* If A is a C^*-algebra, then

$$\|a\|^2 = \|aa^*\| \leq \|a\| \cdot \|a^*\|$$

and arguing as above, we see that the operator $*$ is in fact an isometry; that is, $\|a\| = \|a^*\|$ for all $a \in A$.

Clearly the notion of a C^*-algebra is an abstraction of the properties of the adjoint operator on the space of (topological) endomorphisms of a Hilbert space. This generalization, however, is in some sense vacuous: the Gelfand-Naimark theorem shows that every C^*-algebra is isomorphic to a closed, self-adjoint subalgebra of End(H) for some Hilbert space H by a map that preserves both the complex algebra and metric structures of the corresponding spaces as well as the $*$-operator; that is, by an isometric $*$-isomorphism.

Although we state the next suite of results (through Theorem 2-16) for endomorphisms of Hilbert spaces, the reader should note that in fact only the properties of a C^*-algebra are required.

We now resume the general exposition; we first consider the spectral radius of normal elements of End(H).

2-14 PROPOSITION. *Let $T \in \mathrm{End}(H)$ be normal. Then* $\mathrm{r}(T) = \|T\|$.

PROOF. Since T is normal, $(TT^*)^m = T^m (T^*)^m$ for all nonnegative integers m. Hence applying property (v) above (twice) and Eq. 2.8 to the self-adjoint operator TT^*, we obtain

$$\|T\|^{2^n} = \|TT^*\|^{2^{n-1}} = \|T^{2^n}(T^*)^{2^n}\|^{1/2} = \|T^{2^n}(T^{2^n})^*\|^{1/2} = \|T^{2^n}\| \ .$$

Thus

$$\|T^{2^n}\|^{2^{-n}} = \|T\|$$

for all n, whence $r(T)=\|T\|$ by Theorem 2-6. ❑

2-15 PROPOSITION. *Let* $T\in\text{End}(H)$. *If* T *is unitary, then* $\text{sp}(T)\subseteq S^1$; *if* T *is self-adjoint, then* $\text{sp}(T)\subseteq\mathbf{R}$. (As usual, $S^1=\{z\in\mathbf{C}:|z|=1\}$ is the circle group.)

PROOF. We make two preliminary observations. First, since the adjoint operator is antimultiplicative, an endomorphism of H is invertible if and only if its adjoint is. In particular, given $T\in\text{End}(H)$, $\lambda\cdot 1_H-T$ is invertible if and only if $\overline{\lambda}\cdot 1_H-T^*$ is likewise invertible, and hence $\lambda\in\text{sp}(T)$ if and only if $\overline{\lambda}\in\text{sp}(T^*)$. Second, if $T\in\text{End}(H)$ is itself invertible, then for any nonzero λ,

$$\lambda^{-1}(\lambda\cdot 1_H-T)T^{-1}=-(\lambda^{-1}\cdot 1_H-T^{-1})$$

and it follows that $\lambda\in\text{sp}(T)$ if and only if $\lambda^{-1}\in\text{sp}(T^{-1})$.

Assume now that T is unitary, so that $TT^*=1_H$. By property (v) above, $\|T\|=1$, and so the spectral radius of T is also 1. Noting that $(T^*)^{-1}=T$ and applying our preliminary observations, we deduce that $\lambda\in\text{sp}(T)$ if and only if $\overline{\lambda}^{-1}\in\text{sp}(T)$. Thus if $\lambda\in\text{sp}(T)$, then both λ and λ^{-1} have magnitude bounded by 1, which clearly forces λ to lie in S^1, as claimed.

Finally, assume that T is self-adjoint, and consider the convergent series

$$\exp(iT)=\sum_{n=0}^{\infty}\frac{(iT)^n}{n!}\ .$$

By continuity and conjugate linearity,

$$\exp(iT)^*=\sum_{n=0}^{\infty}\frac{(-iT)^n}{n!}=\exp(-iT)$$

and so $\exp(iT)^*=\exp(iT)^{-1}$. Therefore $\exp(iT)$ is unitary. According to Exercise 5 below, if $\lambda\in\text{sp}(T)$, then $\exp(i\lambda)\in\text{sp}(iT)$, and by the analysis of the unitary case, $|\exp(i\lambda)|=1$. Thus the real part of $i\lambda$ must be zero, which is to say that $\lambda\in\mathbf{R}$. ❑

Recall from the previous section that if A is a commutative Banach algebra, then $\hat{A}$ is the space of characters of A, and $\hat{A}$ admits a compact Hausdorff topology.

2-16 PROPOSITION. *Let* A *be a self-adjoint, unital, closed, commutative subalgebra of* $\text{End}(H)$. *Then the Gelfand transform* $\Gamma:A\to\mathscr{C}(\hat{A})$ *is an isometric isomorphism of unital complex algebras. The map* Γ *is, moreover, a* $*$*-isomorphism in the sense that* $\Gamma(T^*)=\overline{\Gamma(T)}$ *for all* $T\in A$.

PROOF. Note first that every element of A is normal, since A is commutative. Therefore, by Theorem 2-11 and Proposition 2-14, for all $T \in A$,

$$\|T\| = \mathrm{r}(T) = \|\hat{T}\|_\infty$$

is indeed an isometry (hence continuous, injective, and therefore a homeomorphism onto its image).

Suppose that $T \in A$ is self-adjoint. Then by Proposition 2-15,

$$\hat{T}(\gamma) = \gamma(T) \in \mathrm{sp}(T) \subseteq \mathbf{R}$$

for all γ, whence $\hat{T}$ is likewise self-adjoint in the sense that it assumes only real values. Now any arbitrary $T \in A$ can be decomposed into a sum $T = T_0 + iT_1$ where both T_0 and T_1 are self-adjoint and defined as follows:

$$T_0 = \frac{T + T^*}{2} \quad \text{and} \quad T_1 = \frac{T - T^*}{2i} \quad .$$

One sees at once that $T^* = T_0 - iT_1$. Since both $\Gamma(T_0)$ and $\Gamma(T_1)$ are real-valued, we may readily compute that

$$\begin{aligned} \Gamma(T^*) &= \Gamma(T_0 - iT_1) \\ &= \Gamma(T_0) - i\Gamma(T_1) \\ &= \overline{\Gamma(T_0) + i\Gamma(T_1)} \\ &= \overline{\Gamma(T_0 + iT_1)} \\ &= \overline{\Gamma(T)} \quad . \end{aligned}$$

This establishes the second assertion of the proposition.

It remains to show that $\Gamma : A \to \mathscr{C}(\hat{A})$ is surjective, and for this we collect the following facts about $\mathrm{Im}(\Gamma)$:

(i) $\mathrm{Im}(\Gamma)$ contains the constant functions, since A is unital, and $\mathrm{Im}(\Gamma)$ separates points by Theorem 2-11, part (ii).

(ii) $\mathrm{Im}(\Gamma)$ is a self-adjoint subalgebra of $\mathscr{C}(\hat{A})$, since A is self-adjoint in $\mathrm{End}(H)$ and, as we have seen above, $\Gamma(T^*) = \overline{\Gamma(T)}$ for all $T \in A$.

(iii) $\mathrm{Im}(\Gamma)$ is closed in $\mathscr{C}(\hat{A})$, since it is isometrically isomorphic to A.

Thus, in accordance with (i) and (ii), the Stone-Weierstrass theorem (Proposition 2-12) implies that $\mathrm{Im}(\Gamma)$ is dense in $\mathscr{C}(\hat{A})$. Hence from (iii) we deduce that in fact $\mathrm{Im}(\Gamma) = \mathscr{C}(\hat{A})$, and this completes the proof. ❑

The First Spectral Theorem

We now make our last preparations for the first spectral theorem. Assume that $T \in \mathrm{End}(H)$ is normal. Henceforth, A_T shall denote the smallest closed, self-adjoint, unital subalgebra of $\mathrm{End}(H)$ containing T. This is clearly the closure of the algebra generated by 1_H, T, and T^*, and moreover, A_T is commutative because T is normal. We must now distinguish between $\mathrm{sp}(T)$, the spectrum of T computed as usual in the full algebra $\mathrm{End}(H)$, and $\mathrm{sp}_A(T)$, the spectrum of T as computed in the subalgebra A_T. The latter is defined by

$$\mathrm{sp}_A(T) = \{\lambda \in \mathbf{C} : \lambda \cdot 1_H - T \notin A_T^{\times}\} \ .$$

Clearly $\mathrm{sp}(T) \subseteq \mathrm{sp}_A(T)$; the opposite inclusion also holds, as we shall see in the proof of the following theorem. Finally, if W is any nonempty subset of $\mathbf{C}$, we let i_W denote the inclusion map $W \to \mathbf{C}$.

2-17 THEOREM. (The First Spectral Theorem) *Let* $T \in \mathrm{End}(H)$ *be normal, and let* A_T *be defined as above. Then there exists an isometric* $*$*-isomorphism of unital complex algebras* $\Phi : \mathscr{C}(\mathrm{sp}(T)) \to A_T$ *such that* $\Phi(i_{\mathrm{sp}(T)}) = T$.

PROOF. Consider the Gelfand transform of T as defined on the space of characters of A_T:

$$\hat{T} : \hat{A}_T \to \mathbf{C}$$
$$\gamma \mapsto \gamma(T) \ .$$

According to Theorem 2-11, part (i), $\hat{T}$ is a continuous mapping. Moreover, if $\hat{T}(\gamma_1) = \hat{T}(\gamma_2)$, then appealing to Proposition 2-16, we have

$$\gamma_1(T^*) = \overline{\gamma_1(T)} = \overline{\gamma_2(T)} = \gamma_2(T^*) \ .$$

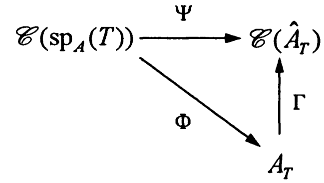
Thus γ_1 and γ_2 agree on the unital subalgebra of $\mathrm{End}(H)$ generated by T and T^*, and hence, by continuity, they also agree on its closure, A_T; that is, $\gamma_1 = \gamma_2$. Therefore $\hat{T}$ is injective, and so by the open mapping theorem a homeomorphism onto its image, which by part (iii) of the previously cited theorem is precisely $\mathrm{sp}_A(T)$. To summarize,

$$\hat{T} : \hat{A}_T \xrightarrow{\sim} \mathrm{sp}_A(T) \ .$$

Next consider the transposed map

$$\Psi : \mathscr{C}(\mathrm{sp}_A(T)) \to \mathscr{C}(\hat{A}_T)$$
$$f \mapsto f \circ \hat{T} \ .$$

This clearly respects conjugation and norm and is therefore an isometric $*$-isomorphism. We now define $\Phi = \Gamma^{-1}\Psi$, so that the following diagram commutes:



Being defined as the composition of isometric $*$-isomorphisms, Φ is again an isometric $*$-isomorphism. We consider its effect on a function $f \in \mathscr{C}(\mathrm{sp}_A(T))$. First note that by definition, $\Psi(f)(\gamma) = f(\gamma(T))$. But since the Gelfand transform is an isomorphism, every map in $\mathscr{C}(\hat{A}_T)$ takes the form $\gamma \mapsto \gamma(P)$ for some unique $P \in A_T$. Thus by the diagram above, we find that $\Phi(f)$ is characterized by the following property:

$$f(\gamma(T)) = \gamma(\Phi(f)) \quad \forall \gamma \in \hat{A}_T \ .$$

From this it is clear that $\Phi(i_{\mathrm{sp}_A(T)}) = T$ and that $\Phi(1) = 1_H$. Thus it only remains to show that $\mathrm{sp}_A(T) = \mathrm{sp}(T)$.

Let $\lambda \in \mathrm{sp}_A(T)$ and choose $f \in \mathscr{C}(\mathrm{sp}_A(T))$ such that f has maximum absolute value 1, $f(\lambda) = 1$, and $f(\mu) = 0$ whenever $|\lambda - \mu| \geq \varepsilon$. Let $P = \Phi(f)$. Then since Φ is an isometry and f is zero away from λ, we have that

$$\begin{aligned}||(T - \lambda \cdot 1_H)P|| &= ||\Phi^{-1}((T - \lambda \cdot 1_H)P)||_\infty \\ &= ||(1_{\mathrm{sp}_A(T)} - \lambda)f||_\infty \\ &\leq \varepsilon \ .\end{aligned}$$

Thus, if $T - \lambda \cdot 1_H$ were invertible, it would follow that

$$\begin{aligned}1 &= ||f||_\infty = ||P|| \\ &= ||(T - \lambda \cdot 1_H)^{-1}(T - \lambda \cdot 1_H)P|| \\ &\leq ||(T - \lambda \cdot 1_H)^{-1}|| \, ||(T - \lambda \cdot 1_H)P|| \\ &\leq ||(T - \lambda \cdot 1_H)^{-1}|| \cdot \varepsilon \ .\end{aligned}$$

But since ε is arbitrary, this forces $\| T-\lambda\cdot 1_H\|$ to infinity. Hence, $T-\lambda\cdot 1_H$ is not invertible, and indeed $\lambda\in \mathrm{sp}(T)$. This completes the proof. ❑

Positive Operators

In this subsection we recall the notion of a positive operator and show, as an easy consequence of the first spectral theorem, that such operators admit "square roots" in an obvious sense to be defined below. As a preliminary we need to introduce a criterion for invertibility that allows us to interpret elements of the spectrum of an operator as generalized eigenvalues.

Again let H be a complex Hilbert space and let $T\in\mathrm{End}(H)$. We say that T is *bounded away from zero* if there exists an $\varepsilon>0$ such that $\|T(x)\|\geq\varepsilon\|x\|$ for all $x\in H$. Note that a map bounded away from zero has trivial kernel and is therefore injective.

2-18 LEMMA. *Let T be an operator in* End(H). *Then the following five statements are equivalent:*

(i) *T is invertible in* End(H).

(ii) *T^* is invertible in* End(H).

(iii) *T and T^* are bounded away from* 0.

(iv) *T and T^* are injective and* Im(T) *is closed in H.*

(v) *T is bijective.*

PROOF. (i)⇔(ii) This follows at once from the antimultiplicativity of the adjoint operator.

(i)⇒(iii) Since $T^{-1}T(x)=x$ for all $x\in H$, it is clear that T is bounded away from zero by $\|T^{-1}\|$. In light of the equivalence between (i) and (ii), T^* is likewise bounded away from zero.

(iii)⇒(iv) We need only show that Im(T) is closed. But for all $x,y\in H$,

$$\|T(x)-T(y)\|=\|T(x-y)\|\geq\varepsilon\|x-y\|$$

for some positive ε. Thus any Cauchy sequence in Im(T) must come from a Cauchy sequence in H and must therefore converge. Hence Im(T) is closed.

(iv) ⇒(v) Consider $T(H)^{\perp}$, the orthogonal complement to $T(H)$ in H. (See Exercises 11 and 12 below.) Since for all $x,y\in H$, $\langle T(x)|y\rangle=\langle x|T^*(y)\rangle$, it follows from positive definiteness that $T(H)^{\perp}=\mathrm{Ker}(T^*)$, which by assumption is trivial.

Consequently, since $T(H)$ is assumed closed, we may conclude by Exercise 13 that $T(H)=(T(H)^{\perp})^{\perp}=H$, as required.

(v) $\Rightarrow$ (i) This is just a special case of the open mapping theorem. ❑

We may use this result to make an explicit connection between the spectrum of an endomorphism and an obvious generalization of the ordinary linear-algebraic notion of an eigenvalue and corresponding eigenvector.

2-19 LEMMA. *Let T be an operator in* End(H) *and let $\lambda \in \mathrm{sp}(T)$. Then there is a sequence of unit vectors $\{x_n\}$ such that either*

(i) $\|T(x_n)-\lambda x_n\| \to 0$ *or*

(ii) $\|T^*(x_n)-\overline{\lambda}\, x_n\| \to 0$.

PROOF. If both alternatives fail, then clearly $T-\lambda 1_H$ and its adjoint are bounded away from 0 and therefore invertible, by Lemma 2-18. But this contradicts the assumption that $\lambda \in \mathrm{sp}(T)$. ❑

2-20 PROPOSITION. *Let T be a normal operator in* End(H), *and again suppose that $\lambda \in \mathrm{sp}(T)$. Then for every positive ε there exists a unit vector $x \in H$ such that $\|T(x)-\lambda x\| < \varepsilon$. If λ is isolated in* sp(T), *then in fact λ is an eigenvalue of T.*

PROOF. According to the previous lemma, for arbitrary $T \in \mathrm{End}(H)$, the first statement must at least hold for one of T or T^*. But since T is assumed normal, and therefore so is $T-\lambda \cdot 1_H$, it follows from Exercise 14 that this statement certainly does hold for T.

To prove the second statement, we make use of the isometric isomorphism Φ described in the first spectral theorem. Let λ be an isolated point of the compact subset sp(T). Then we can define a continuous function f from sp(T) to **C** such that $f(\lambda)=1$, while f vanishes identically elsewhere in sp(T). Then by construction and by Theorem 2-17,

$$0 = \|(\lambda \cdot 1 - 1_{\mathrm{sp}(T)}) \cdot f\|_\infty = \|(\lambda \cdot 1_H - T) \circ \Phi(f)\| \ .$$

Here 1 denotes the constant function 1 on sp(T); note also that the infinity norm is computed over sp(T), not **C**. Since f is not the zero map, neither is $\Phi(f)$, whence there exists a nonzero $x \in H$ such that $(\lambda \cdot 1_H - T)x = 0$. Thus λ is an eigenvalue for T, as claimed. ❑

A self-adjoint operator $T\in\text{End}(H)$ is called a *positive* operator if $\langle T(x)|x\rangle\geq 0$ for all $x\in H$. If this is the case, we write $T\geq 0$. Clearly for all $T\in\text{End}(H)$ the product TT^* is positive.

2-21 PROPOSITION. *A normal operator T is self-adjoint if and only if* $\text{sp}(T)\subseteq\mathbf{R}$ *and positive if and only if* $\text{sp}(T)\subseteq\mathbf{R}_+$.

PROOF. We know that a self-adjoint operator has real spectrum by Proposition 2-15. Assume, moreover, that T is positive, and let $\lambda\in\text{sp}(T)$. According to the previous proposition, for every $\varepsilon>0$ there exist vectors x and y in H such that x is a unit vector, y has norm less than ε, and $T(x)=\lambda x+y$. Thus

$$0\leq\langle T(x)|x\rangle=\langle\lambda x+y|x\rangle=\lambda\langle x|x\rangle+\langle y|x\rangle=\lambda+\langle y|x\rangle\ .$$

It follows from the Cauchy-Schwarz inequality that $0\leq\lambda+\varepsilon$. Since ε is arbitrary, λ cannot be negative.

Now assume that the spectrum of T is real. Then the mapping $i_{\text{sp}(T)}$ is self-adjoint, whence so is T by the first spectral theorem. If, moreover, the spectrum of T is nonnegative, then we may of course define the continuous function $f(\lambda)=\sqrt{\lambda}$ on $\text{sp}(T)$, which corresponds to the self-adjoint operator $\Phi(f)$. Accordingly,

$$\langle T(x)|x\rangle=\langle\Phi(f)^2(x)|x\rangle=\langle\Phi(f)(x)|\Phi(f)(x)\rangle\geq 0$$

as required. ❑

2-22 PROPOSITION. *Let T be a positive operator in* End(H). *Then there exists a unique positive operator $T^{1/2}\in\text{End}(H)$ such that $(T^{1/2})^2=T$. Moreover, $T^{1/2}$ commutes with every operator that commutes with T.*

PROOF. Let f be as in the proof of the previous result and define $T^{1/2}=\Phi(f)$, so that clearly $(T^{1/2})^2=T$. By the Stone-Weierstrass theorem f may be expressed as a uniformly convergent power series in the function $1_{\text{sp}(T)}$ on $\text{sp}(T)$, whence $T^{1/2}$ may be expressed as a uniformly convergent power series in T. Thus $T^{1/2}$ indeed commutes with every operator that commutes with T. Uniqueness is established in Exercise 15 below. ❑

The Second Spectral Theorem

In this subsection we state, without proof, the second spectral theorem. As a prerequisite we must first introduce the notion of a spectral measure.

Note that although we state this result in integral form, it is in fact an extension of the first spectral theorem to the class of bounded complex Borel func-

tions on the spectrum of a given normal operator. We shall return to this point briefly below.

Let H be a Hilbert space, and let $\langle X, \mathfrak{M} \rangle$ be a measurable space (cf. Section 1.2). Then a *spectral measure* on X taking values in the operator space End(H) is a mapping $E: \mathfrak{M} \rightarrow \mathrm{End}(H)$ satisfying the following axioms:

(i) For all $Y \in \mathfrak{M}$, $E(Y)$ is an orthogonal projection in End(H) onto a closed subspace.

(ii) The full space X corresponds to the identity map, and the empty set corresponds to the zero map; i.e., $E(X) = 1_H$, and $E(\varnothing) = 0$.

(iii) For all $Y_1, Y_2 \in \mathfrak{M}$, $E(Y_1 \cap Y_2) = E(Y_1)E(Y_2)$.

(iv) Let $\{Y_n\}$ be a countable collection of measurable sets. Then

$$E(\bigcup Y_n) = \bigvee E(Y_n)$$

where the right-hand side denotes projection onto the closed subspace generated by the union of the images of the $E(Y_n)$.

Recall that a *signed measure* is a map from $\mathfrak{M}$ to $\mathbf{R} \cup \{\pm\infty\}$ that is additive on countable unions of disjoint measurable sets and takes at most one of the values $\pm\infty$. According to the Hahn decomposition theorem, every signed measure μ may be written as a difference of ordinary (nonnegative) measures μ^+ and μ^- that are mutually singular; that is, X is the disjoint union of two measurable sets X^+ and X^- such that μ^+ is trivial on X^-, and μ^- is trivial on X^+. Hence integration with respect to μ may be defined in the natural way as the difference of two integrals defined with respect to μ^+ and μ^-. A *complex measure* is a sum $\mu_0 + i\mu_1$ of two signed measures μ_0 and μ_1 that do *not* take the values $\pm\infty$. Integration with respect to a complex measure is again readily defined.

One verifies easily that a spectral measure E on X gives rise to a family of ordinary measures μ_x on X ($x \in H$): for $Y \in \mathfrak{M}$, define

$$\mu_x(Y) = \langle E(Y)x \,|\, x \rangle \ .$$

For all $x \in H$, this measure is clearly bounded by $\|x\|^2$, owing to axiom (i) for a spectral measure. These measures μ_x in turn give rise to a doubly indexed family of complex measures $\mu_{x,y}$ on X ($x,y \in H$) defined by

$$\mu_{x,y} = \frac{1}{4} \sum_{k=1}^{4} i^k \mu_{x+i^k y}$$

or equivalently,

$$\mu_{x,y}(Y) = \langle E(Y)x | y \rangle \ .$$

Now let f be a bounded, measurable, complex-valued function on X, and consider the associated integral

$$I_f(x,y) = \int_X f(\lambda) d\mu_{x,y}(\lambda) \ .$$

This is clearly a sesquilinear form on H (i.e., linear in the first variable, conjugate linear in the second) and continuous on $H \times H$, because f is bounded by $\|f\|_\infty$ while the measures $\mu_{x+i^k y}$ are bounded by $\|x+i^k y\|^2$. Hence by Exercise 9, there exists an endomorphism T_f on H such that

$$\begin{aligned} \langle T_f(x) | y \rangle &= I_f(x,y) \\ &= \int_X f(\lambda) d\mu_{x,y}(\lambda) \ . \end{aligned}$$

One often expresses this more succinctly as an "operator integral," as follows:

$$T_f = \int_X f(\lambda) dE(\lambda)$$

and this is henceforth the implicit meaning attached to such an integral. With this in mind we can now state the second spectral theorem (for normal operators).

2-23 THEOREM. (The Second Spectral Theorem) *Let T be a normal operator in* End(H). *Then there exists a spectral measure E defined on the Borel subsets of* sp(T) *such that*

$$T = \int_{\mathrm{sp}(T)} \lambda dE(\lambda) \ .$$

That is, for all $x, y \in H$,

$$\langle T(x) | y \rangle = \int_{\mathrm{sp}(T)} \lambda d\mu_{x,y}(\lambda)$$

where $\mu_{x,y}$ is the complex measure associated with E. Moreover, for every Borel subset Y of sp(T), *the associated projection $E(Y)$ commutes with every operator that commutes with T.*

While we will not prove this, we will at least say how a spectral measure E on sp(T) is naturally associated with the normal operator T. Let Y be any Borel subset of sp(T). Then the characteristic function χ_Y from sp(T) to **C** is certainly Borel measurable. Via an extension of the first spectral theorem, χ_Y corresponds to an operator $E(Y)$ in End(H), which turns out to be a projection that commutes with every operator that commutes with T. The association $Y \mapsto E(Y)$ is in fact the required spectral measure.

2.4 Unitary Representations

In this brief section we develop some basic facts about a special class of topological representations, the so-called unitary representations. We shall use the first spectral theorem to prove a powerful topological extension of Schur's lemma, a well-known result in the ordinary theory of group representations.

We begin working over a pre-Hilbert space H. One can show by routine methods that $\hat{H}$, the metric completion of H, also admits a compatible structure as a pre-Hilbert space, which is by construction in fact a full Hilbert space. Moreover, any bounded operator on H likewise extends uniquely by continuity to a bounded operator on $\hat{H}$. Hence adjoint operators are also defined for H by restricting the adjoint defined on the completion.

Assuming that H is a pre-Hilbert space with respect to some given positive Hermitian form $\langle\,|\,\rangle$, a bounded endomorphism T of H is called *pre-unitary* (with respect to the given form) if, as one would expect, the following equation holds for all $x,y \in H$:

$$\langle x,y\rangle = \langle T(x),T(y)\rangle \quad . \tag{2.9}$$

Equivalently, $TT^* = 1_V$, where T^* again denotes the adjoint of T. A pre-unitary endomorphism on a Hilbert space is, of course, a unitary operator in the usual sense.

More generally, if H and H' are pre-Hilbert spaces, we shall call an isomorphism $T: H \cong H'$ *pre-unitary* if Eq. 2.9 holds.

DEFINITION. If (ρ,H) is a representation of a locally compact group G on a pre-Hilbert space H, we say that ρ is *pre-unitary* if each topological automorphism ρ_g ($g \in G$) is pre-unitary; that is, if

$$\langle u,v\rangle = \langle \rho_g(u),\rho_g(v)\rangle \quad .$$

We also say that the underlying form $\langle\,|\,\rangle$ is *invariant under* $\rho(G)$.

DEFINITION. Two arbitrary topological representations (ρ,H) and (ρ',H') are called *pre-unitarily equivalent* if there exists a pre-unitary topological isomorphism $T:H\cong H'$ such that $T\circ\rho_g=\rho'_g\circ T$ for all $g\in G$.

In the context of these definitions, if H and H' are moreover Hilbert spaces, we then speak, respectively, of *unitary representations* and *unitary equivalences.*

2-24 PROPOSITION. *Let H and H' be two Hilbert spaces. If two unitary representations* (ρ,H) and (ρ',H') *are equivalent, then they are moreover unitarily equivalent.*

PROOF. Let $T:H\to H'$ be the topological G-isomorphism defining the equivalence of (ρ,H) and (ρ',H'). Define $T^*:H'\to H$ by the relation

$$\langle T^*(x)|y\rangle = \langle x|T(y)\rangle$$

for all $x\in H'$, $y\in H$. (Again see Exercises 9 and 10; note that this slight generalization of the adjoint has all of the usual formal properties.) Then one shows easily that TT^* is a positive operator on H'. According to Proposition 2-22, there exists a unique positive (in particular, self-adjoint) operator U such that $U^2=TT^*$ and U (hence U^{-1}) commutes with every operator that commutes with TT^*. An easy calculation shows that the composite operator $U^{-1}T$ is unitary:

$$(U^{-1}T)(U^{-1}T)^* = U^{-1}TT^*(U^{-1})^* = U^{-1}TT^*U^{-1} = U^{-1}U^2U^{-1} = 1_H \ .$$

It remains to show that $U^{-1}T$ also defines an equivalence between the unitary representations (ρ,H) and (ρ',H'). This follows trivially, provided that U^{-1} commutes with ρ'_g for all $g\in G$, and for this it suffices to show that TT^* commutes with the ρ'_g. To establish this last assertion, we begin with the defining relation

$$T\rho_g = T\rho'_g \ .$$

Taking the adjoint of both sides (and noting that both representations are, by assumption, unitary), we have

$$\rho_g T^* = T^*\rho'_g$$

whence

$$TT^*\rho'_g = T\rho_g T^* = \rho'_g\ TT^* \ .$$

This completes the proof. ❑

We come now to one of the principal results of the present chapter: Schur's lemma. This is an extension to our topological setting of a most elegant result for abstract group representations. We give two proofs of the "difficult part," one based only on the first spectral theorem, proven above in its entirety, and the other given as an illustration of how the second spectral theorem may be applied.

The key to the first proof is the following immediate consequence of the first spectral theorem.

2-25 PROPOSITION. *Let T be a normal operator on a complex Hilbert space H, and, as usual, let A_T be the closure of the unital subalgebra of* End(H) *generated by T and T^*. Then the following three statements are equivalent:*

(i) sp(T) *is a point.*

(ii) $A_T = \mathbf{C}$.

(iii) *T is a scalar multiple of the identity operator.* ☐

This brings us directly to the main event.

2-26 THEOREM. (Schur's Lemma).

(i) *Let G be an arbitrary group, and let V and V' be vector spaces over an arbitrary field. Suppose that both ρ and ρ' are algebraically irreducible representations of G on V and V', respectively. If $T \in$* $\mathrm{Hom}_G(V, V')$, *the space of all G-linear maps from V to V', then either T is the trivial map or T is an algebraic isomorphism.*

(ii) *Assume further that G is a locally compact topological group and that H is a complex Hilbert space. Let ρ be a topologically irreducible unitary representation of G on H, and let $T \in \mathrm{End}_G(H)$, the space of continuous G-linear maps from H to itself. If T is a normal operator, then T is a scalar multiple of the identity map. In particular, for arbitrary $T \in \mathrm{End}_G(H)$, the product T^*T is scalar.*

PROOF. (i) By hypothesis, both V and V' admit no nontrivial, proper G-invariant subspaces. Accordingly, if T is not surjective, it has trivial image, and if T is not injective, its kernel is all of V. Thus if T is not an isomorphism, it is indeed trivial, as claimed. Note well that this argument holds for arbitrary abstract group representations, independent of ground field or topology.

(ii) Certainly we may assume that H is nontrivial. Let the representation $\rho: G \rightarrow \mathrm{End}(H)$ be given as stated, and let T be a normal operator commuting

with ρ. Suppose that $\lambda \in \mathrm{sp}(T)$. Then we can find a nonzero function f on sp(T) that vanishes on an open neighborhood of λ in sp(T). Let $\Phi : \mathscr{C}(\mathrm{sp}(T)) \to A_T$ again be the isometry of the first spectral theorem. Then W, the closure of the subspace $\Phi(f)H$ in H, is invariant under $\rho(G)$; to see this, express $\Phi(f)$ as a limit of polynomials in T, which evidently commute with ρ_g, for all $g \in G$. It follows now from the irreducibility of ρ and the nontriviality of f that in fact $W=H$.

Now suppose that sp(T) is not a singleton. Then we may find another continuous function h with complementary support vis-à-vis f. But then

$$\{0\} = \Phi(h)\Phi(f)H$$

and W cannot be all of H. This contradiction shows that sp(T) must contain no more than one point, and hence the previous proposition applies to complete the proof. ❑

ALTERNATIVE PROOF OF THE SECOND PART. We give this alternative proof based on the second spectral theorem only for positive operators, leaving the extension to arbitrary normal operators to the reader.

Let T be a positive operator on H, whence $\mathrm{sp}(T) \subseteq \mathbf{R}_+$. By the second spectral theorem, there exists a spectral measure E defined on the Borel subsets of sp(T) such that

$$T = \int_{\mathrm{sp}(T)} \lambda dE(\lambda) \quad .$$

Moreover, E has a crucial property: each projection $E(Y)$ commutes with every operator that commutes with T and, in particular, commutes with every ρ_g, since T is a G-endomorphism and ρ is unitary. Thus the image of each $E(Y)$ is a G-invariant subspace of H and therefore, by assumption, is either the trivial subspace or H itself, which is to say that for every Borel subset Y, the endomorphism $E(Y)$ is either the trivial projection or the identity projection.

Let us now unwind the previous equation. For all $x, y \in H$, we have

$$\begin{aligned}
\langle Tx, y\rangle &= \int_{\mathrm{sp}(T)} \lambda d\mu_{x,y}(\lambda) \\
&= \frac{1}{4}\sum_{k=1}^{4} i^k \int_{\mathrm{sp}(T)} \lambda d\mu_{x+i^k y}(\lambda) \\
&= \frac{1}{4}\sum_{k=1}^{4} i^k \sup_{\psi} \int_{\mathrm{sp}(T)} \psi(\lambda) d\mu_{x+i^k y}(\lambda)
\end{aligned}$$

where for each term, the supremum is taken over all simple functions ψ on sp(T) such that $\psi(\lambda)\leq\lambda$. Accordingly,

$$\begin{aligned}\langle Tx, y\rangle &= \frac{1}{4}\sum_{k=1}^{4} i^k \sup\sum_j \inf(Y_j)\langle E(Y_j)(x+i^k y)|(x+i^k y)\rangle \\ &= \frac{1}{4}\sum_{k=1}^{4} i^k \sup\sum_j \inf(Y_j)\,\delta_j\cdot\langle (x+i^k y)|(x+i^k y)\rangle \\ &= \sup\sum_j \inf(Y_j)\,\delta_j \cdot \frac{1}{4}\sum_{k=1}^{4} i^k\langle (x+i^k y)|(x+i^k y)\rangle \\ &= \langle \lambda_0 x, y\rangle\end{aligned}$$

where each supremum is taken over all finite, disjoint measurable covers $\{Y_j\}$ of sp(T), and δ_j is either 0 or 1 depending on whether $E(Y_j)$ is the zero projection or the identity projection. Thus $T=\lambda_0\cdot 1_H$, as claimed. ❑

REMARKS. (i) Suppose that in the second part H is assumed finite-dimensional. Then we can give a direct proof based on elementary linear algebra that for any $T\in\mathrm{End}_G(H)$, the product T^*T is scalar. We know that T^*T is a self-adjoint operator on H, and so by the spectral decomposition theorem, H decomposes into the direct sum of closed orthogonal eigenspaces with respect to T^*T. Let W be the eigenspace belonging to the eigenvalue λ. Then for $w\in W$ and $g\in G$,

$$T^*T(\rho_g(w)) = \rho_g(T^*T(w)) = \rho_g(\lambda w) = \lambda\rho_g(w)$$

so that $\rho_g(w)$ again lies in the eigenspace belonging to λ. It follows that W is a nontrivial, closed, G-invariant subspace of V. Since ρ is assumed irreducible, in fact $W=H$, and therefore $T^*T=\lambda\cdot 1_H$.

(ii) One key step in the proof of Schur's lemma is noteworthy even when G is trivial: every normal operator on a Hilbert space H of dimension greater than one leaves a nontrivial, proper, closed subspace $W\subseteq H$ invariant. When H is finite-dimensional, this follows from the existence of eigenvectors, but these need not occur in the infinite-dimensional case. Thus some of the analysis on Hilbert spaces that we have here developed is certainly unavoidable. Suffice it to note further that there need *not* be invariant subspaces W in a general Banach space V, even for nice operators. For instance, $\mathbf{Z}$ admits an infinite-dimensional, norm-preserving Banach representation that is in fact irreducible!

We conclude this section with a final application of these spectral techniques to prove a theorem that provides a natural bridge into the next topic.

2-27 THEOREM. *Let G be a locally compact abelian group and let* (ρ, H) *be an irreducible unitary representation of G on a Hilbert space H. Then* $\dim_{\mathbf{C}}(H) = 1$.

PROOF. For every $g \in G$, the corresponding unitary (hence normal) transformation ρ_g lies in $\mathrm{End}_G(H)$ and hence, by Schur's lemma, acts by a scalar, say, $\chi(g) \in S^1$. Hence each nonzero $x \in H$ generates the G-invariant closed subspace $\mathbf{C}x$, which must then be H itself, since ρ is assumed irreducible. ❑

Note in the proof that since ρ is a representation of G, the map χ is continuous from G into S^1, with the further property that

$$\chi(gg') = \chi(g)\chi(g')$$

for all $g, g' \in G$. This qualifies χ as a *(unitary) character* of G, and such characters are very much at center stage in the following chapter.

Exercises

1. Let V be a topological space that is also a vector space over the topological field k. Show that V is a topological vector space over k if and only if the following maps are continuous:

$$\begin{array}{ll} V \times V \to V & \qquad k \times V \to V \\ (v,w) \mapsto v + w & \qquad (\lambda, v) \mapsto \lambda v \end{array}$$

2. Let A be a (complex) Banach algebra, possibly without unity. Show that A embeds isometrically into a Banach algebra A' with unity. [*Hint*: Consider the direct product $A \times \mathbf{C}$; there is only one way to extend the ring structures of A and $\mathbf{C}$ to this product. For the norm, set $\|(a, \lambda)\| = \|a\| + |\lambda|$, where the latter is, of course, the ordinary complex absolute value.]

3. Let A be a Banach algebra with unity. Show that we may replace the given norm $\|\cdot\|$ on A with another norm $\|\cdot\|_1$ that yields the identical metric topology, with the further property that $\|1\|_1 = 1$. [*Hint*: For each $a \in A$, let ρ_a denote the left multiplication map and define $\|a\|_1 = \|\rho_a\|$, the norm of the associated linear transformation.]

4. Let A be a Banach algebra and let $a \in A$ satisfy $\|a\| < 1$. Show that for all integers m and n with $1 \le m < n$,

$$\left\| \sum_{j=m+1}^{n} a^j \right\| \leq \frac{\|a\|^{m+1}}{1-\|a\|} .$$

Conclude that the series $\Sigma_{j=0}^{\infty} a^j$ converges in A.

5. Let A be a complex unital Banach algebra and let $a \in A$. Let D denote the closed disk in the complex plane of radius $\|a\|$. Assume that $f(z)$ is holomorphic in a region containing D (and hence, by elementary complex analysis, has a valid power series expansion on D). Show (i) that $f(a)$ converges in A and (ii) that if $\lambda \in \text{sp}(a)$ and $\lambda \in D$, then $f(\lambda) \in \text{sp}(f(a))$.

6. Let A be a complex unital Banach algebra and let $x,y \in A$.

(a) Show that if $1-xy$ is invertible, then so is $1-yx$. [*Hint*: Suppose that z is the inverse of $1-xy$. Show that $xyz=zxy$ and deduce that $1+yzx$ is the required inverse for $1-yx$.]

(b) Deduce from part (a) that if λ is a nonzero element in the spectrum of xy, then λ is likewise in the spectrum of yx. Show that restriction of this statement to nonzero elements of the spectrum is in fact necessary.

(c) Conclude from parts (a) and (b) that if x is invertible, then the spectrum of xy is identical to that of yx for all $y \in A$.

7. Let A be a complex unital Banach algebra and let $x,y \in A$. Show that xy and yx have the same spectral radius. [*Hint*: Use the previous exercise.]

8. Let A be a complex Banach algebra *without* unity, and suppose that A embeds isometrically into a unital Banach algebra B as a subspace of codimension 1. (According to Exercise 2, such an algebra B always exists.)

(a) Show that linear extension and restriction define a pair of inverse mappings between the character spaces $\hat{A}$ and $\hat{B}$.

(b) Let $\Gamma_B : B \to \mathscr{C}(\hat{B})$ denote the Gelfand transform for B. Show that the image of A under Γ_B already separates points in $\hat{B}$ and hence in $\hat{A}$. (See Theorem 2-11.)

9. Let H be a Hilbert space. Show that every element of $\varphi \in H^*$ takes the form

$$\varphi(x) = \langle x | x_0 \rangle$$

for some element $x_0 \in H$ uniquely defined by φ. [*Hint*: Assume that φ is not the zero transformation and let K denote the kernel of φ. Decompose H into the direct sum of K and $K^\perp$ (the closed subspace of H consisting of elements orthogonal to K). Clearly there exists $y_0 \in K^\perp$ such that $\varphi(y_0)=1$. Now show that $x_0=y_0/\|y_0\|$ has the required property. The key will be that $x-\varphi(x)y_0$ lies in K for all $x \in H$.]

10. Let H be a Hilbert space and let $T \in \mathrm{End}(H)$. Show that the adjoint transformation $T^* \in \mathrm{End}(H)$ exists and is unique. [*Hint*: For each $y \in H$, the mapping $x \mapsto \langle T(x)|y\rangle$ lies in H^*. Hence by the previous exercise there exists an element $T^*(y) \in H$ such that $\langle T(x)|y\rangle = \langle x|T^*(y)\rangle$ for all $x \in H$. Now show that T^* lies in End(H).]

11. Let X be a subset of a Hilbert space H and define $X^\perp$ to be the set of points in H orthogonal to every element of X. Show that $X^\perp$ is a closed subspace of H.

12. Let W be a closed subspace of a Hilbert space H and define $W^\perp$ as in the previous problem. Show that $H = W \oplus W^\perp$ as a vector space. [*Hint*: Given $x \in H$ define $\mathrm{pr}_W(x)$, the *orthogonal projection* of x onto the subspace W, to be the closest point of W to x. Then show that $x = \mathrm{pr}_W(x) + (x-\mathrm{pr}_W(x))$ is the required unique decomposition.]

13. Continuing in the context of the previous problem, show that $(X^\perp)^\perp$ is the smallest closed subspace of H that contains the closure of X. Conclude, in particular, that if W is a closed subspace of H, then $(W^\perp)^\perp = W$.

14. Let H be a Hilbert space and let T be a normal element of End(H). Show that for all $x \in H$, $\|T(x)\| = \|T^*(x)\|$. [*Hint*: By definition of the adjoint, for all $x \in H$, $\langle T(x)|T(x)\rangle = \langle T^*T(x)|x\rangle$. But T^* commutes with T.]

15. Let $T \in \mathrm{End}(H)$ be a positive operator on a Hilbert space H. Show that the "square root" of T as defined in Proposition 2-22 is unique, arguing as follows:

(a) Show that if $S \in \mathrm{End}(H)$ is a positive operator such that $S^2=T$, then both T and $T^{1/2}$ lie in A_S, the smallest closed, self-adjoint, unital subalgebra of End(H) containing S.

(b) Show that $T^{1/2}$ corresponds under the isomorphism of Theorem 2-17 to a function $g \in \mathscr{C}(\mathrm{sp}(S))$ satisfying $g^2(\lambda)=\lambda^2$ for all $\lambda \in \mathrm{sp}(S)$.

(c) Conclude from (b) and the positivity of S that in fact $S=T^{1/2}$.

16. (Unitarizability for Compact Groups) Let π be a representation of a compact group G on a finite-dimensional vector space V. Show that there exists a scalar product $\langle \, | \, \rangle$ on V that is $\pi(G)$-invariant; that is, π is unitary with respect to the Hilbert space structure defined on V by this scalar product. Note that this construction applies to any finite group with the discrete topology. [*Hint*: Pick any scalar product $[\, | \,]$ on V, and consider the average

$$\langle v \,|\, v' \rangle = \frac{1}{\mathrm{vol}(G)} \int_G [\pi(g)v \,|\, \pi(g)v']\, dg$$

where dg is the Haar measure on G.]

17. Give an example of a finite-dimensional representation of a locally compact, but noncompact, group for which the conclusion asserted by the previous exercise does not hold. [*Hint*: Try $G=\mathrm{SL}_2(\mathbf{C})$, $V=\mathbf{C}^2$, with π taken to be the standard representation.]

18. Let (π, V) be a finite-dimensional unitary representation of a locally compact group G. Show that π is completely reducible; that is, there exists a direct sum decomposition

$$V = \oplus_{i=1}^{r} V_i$$

such that (i) $\pi(G)$ preserves each V_i, and (ii) the restriction of π to V_i is irreducible for all i. [*Hint*: Take orthogonal complements of invariant subspaces.]

19. Give an example of an infinite-dimensional unitary representation of a locally compact group G that is *not* completely reducible. [*Hint*: Try $G=\mathbf{R}$ and $V=L^2(\mathbf{R})$, where π acts by translation on the functions that constitute V.]

20. (Orthogonality Relations for Compact Groups) Let (π, V) and (π', V') be nonisomorphic, irreducible, unitary representations of a *compact* group G. Show that the following identity holds for all $v_1, v_2 \in V$ and $v'_1, v'_2 \in V'$:

$$\int_G \langle \pi(v_1) | v_2 \rangle \langle \pi(v'_1) | v'_2 \rangle' dg = 0$$

where dg denotes the Haar measure on G normalized to give total volume one—this is called the *probability measure* on G—and $\langle \, | \, \rangle$ and $\langle \, | \, \rangle'$ denote the invariant scalar products on V and V', respectively.

21. Let (π, V) be an irreducible unitary representation of a *compact* group G with Haar measure dg. Verify the following identity for all $v_1, v_2, v_3, v_4 \in V$:

$$\int_G \langle \pi(g)v_1 | v_2 \rangle \overline{\langle \pi(g)v_3 | v_4 \rangle}\, dg = \frac{1}{\dim(V)} \langle v_1 | v_2 \rangle \overline{\langle v_3 | v_4 \rangle} \ .$$

22. Let G be a locally compact group with Haar measure dg. Define $L^2(G)$ to be the Hilbert space of square-integrable functions on G; that is, $L^2(G)$ consists of the measurable functions $f: G \to \mathbf{C}$ such that

$$\int_G |f(g)|^2 \, dg < \infty \ .$$

Show that the right (or left) translation action of G on $L^2(G)$ defines a unitary representation relative to the scalar product

$$\langle f | h \rangle = \int_G f(g) \overline{h(g)}\, dg \ .$$

This is called the *regular representation* of G.

23. Let (π, V) be a finite-dimensional unitary representation of a *compact* group G. For any pair (v_1, v_2) of vectors in V, define the associated *matrix coefficient* to be the function $G \to \mathbf{C}$ defined by

$$g \mapsto \langle \pi(g)v_1 | v_2 \rangle$$

where $\langle \ | \ \rangle$ denotes the π-invariant inner product on V.

(a) Show that the *character* $\chi_\pi: G \to \mathbf{C}$ defined by $g \mapsto \operatorname{tr} \pi(g)$ is a linear combination of matrix coefficients (relative to a basis of V). Show further that

$$\chi_\pi(g) = \overline{\chi_\pi(g^{-1})}$$

for all $g \in G$.

(b) (Orthogonality of Characters) Show that if (π', G') is another finite-dimensional unitary representation and if, moreover, π and π' are irreducible, then

$$\chi_\pi * \chi_{\pi'} = \begin{cases} 0 & \text{if } \pi \not\cong \pi' \\ \dfrac{1}{\dim V}\chi_\pi & \text{if } \pi \cong \pi' \end{cases} .$$

Here $*$ denotes the convolution product:

$$f * h(x) = \int_G f(xy^{-1})h(y)dy .$$

24. Assume that G is a compact matrix group; that is, a compact subgroup of $\mathrm{GL}_n(\mathbf{C})$. Let $\mathcal{M}(G)$ denote the $\mathbf{C}$-linear span of the matrix coefficients of all finite-dimensional unitary irreducible representations (π,V) of G. One endows $\mathcal{M}(G)$ with an algebra structure via the tensor product.

(a) Show that the elements of $\mathcal{M}(G)$ are continuous and that $\mathcal{M}(G)$ contains the constant functions and separates points.

(b) Show that $\mathcal{M}(G)$ is uniformly dense in the space of continuous functions from G to $\mathbf{C}$.

(c) Show that $\mathcal{M}(G)$ is dense for the L^2-norm in $L^2(G)$. This is defined by

$$\|f\|_2 = \left\{ \int_G |f(g)|^2 \, dg \right\}^{1/2} .$$

25. Again let G be a compact matrix group.

(a) Show that we have the following decomposition of the (right) regular representation:

$$L^2(G) \cong \hat{\bigoplus_{(\pi,V)\in\hat{G}}} \dim(V)\cdot V$$

where $\hat{G}$ denotes the set of inequivalent irreducible unitary representations of G, and $\hat{\oplus}$ denotes the Hilbert direct sum; that is, the completion of the algebraic direct sum.

(b) If G is *finite*, show that there is a natural identification of $L^2(G)$ with the complex group algebra $\mathbf{C}G$.

26. Show that every irreducible unitary representation of a compact matrix group is necessarily finite-dimensional.

REMARK. The assertions of the preceding three exercises are in fact true for *any* compact group G (that is, without assuming that G is a matrix group). Together they are the content of the Peter-Weyl theorem, the most fundamental result in the representation theory of compact groups.

27. Let G be a locally compact group, and let H be a closed, unimodular subgroup. This means that the left and right Haar measures on H are identical, after appropriate normalization. Let W be a Hilbert space with its corresponding space of unitary transformations denoted $\mathscr{U}(W)$, and suppose that $\sigma: H \to \mathscr{U}(W)$ is a unitary representation of H. Define

$$\mathrm{Ind}_H^G(\sigma)$$

the so-called representation of G *induced by* (σ, W) to be the space of functions f from G to W such that

(i) $f(hg) = \sigma(h)f(g)$ for all $h \in H$, $g \in G$, and

(ii) f is measurable and in L^2 modulo H; that is, the product $\langle f(g) | f(g) \rangle$, which by the previous condition and the unitarity of σ is well-defined on $H \backslash G$, is integrable over the quotient space.

Note that G acts on $\mathrm{Ind}_H^G(\sigma)$ by right translation; that is, by the action

$$(x, f) \mapsto (g \mapsto f(gx))$$

for all $g, x \in G$.

(a) Show that $\mathrm{Ind}_H^G(\sigma)$ is a unitary representation of G. [*Hint*: First show that

$$\overline{dg} = \frac{dg}{dh}$$

is a right G-invariant measure on the homogeneous space $H \backslash G$; use it and the H-invariant scalar product on W to define an appropriate scalar product on $\mathrm{Ind}_H^G(\sigma)$.]

(b) If H is not unimodular, how should the definition of $\mathrm{Ind}_H^G(\sigma)$ be modified to ensure unitarity?

(c) Show that if G is a *finite* group, then there is a natural G-isomorphism

$$\mathrm{Ind}_H^G(\sigma) \cong W \otimes_{\mathbf{C}H} \mathbf{C}G \ .$$

Note that the object on the right is the usual induced module in the representation theory of finite groups.

28. Let $G=\mathbf{R}$, here viewed as an additive, locally compact group with Haar measure given by the ordinary Lebesgue measure dx.

(a) Given $f \in L^2(\mathbf{R})$ and $z \in \mathbf{R}$, define $(\rho_z f)(x) = f(x+z)$. Show that

$$\begin{aligned} \mathbf{R} &\to \mathrm{Aut}(L^2(\mathbf{R})) \\ z &\mapsto \rho_z \end{aligned}$$

is a well-defined unitary representation.

(b) Show that for $z \in \mathbf{R}$, the operator ρ_z has a *purely continuous spectrum*; that is, for each $\lambda \in \mathrm{sp}(\rho_z)$, there exists no corresponding eigenvector, which in turn is to say, no element $f \in L^2(\mathbf{R})$ such that $\rho_z f - \lambda f = 0$.

(c) Determine $\mathrm{sp}(\rho_z)$ and the spectral measure E on $\mathrm{sp}(\rho_z)$, as in the second spectral theorem.

(d) Show that $\mathrm{End}_{\mathbf{R}}(L^2(\mathbf{R}))$ is commutative. [When this happens, one says that the representation $(\rho, L^2(\mathbf{R}))$ is *multiplicity-free*.] Show nonetheless that $\mathrm{End}_{\mathbf{R}}(L^2(\mathbf{R}))$ is not $\mathbf{C}$, so that the representation is not irreducible.

(e) After studying Chapter 4, do this problem again for $G = \mathbf{Q}_p$.

3
Duality for Locally Compact Abelian Groups

For a locally compact abelian group G, its group $\hat{G}$ of characters (i.e., continuous homomorphisms from G to S^1) also acquires the structure of a topological group. In this chapter, we give two distinctive characterizations of what turns out to be the same underlying topology for $\hat{G}$ and examine this topology in detail. The main result is the Pontryagin duality theorem, which says in effect that G and $\hat{G}$ are mutually dual, both algebraically *and* topologically. To prove this, we build upon the results of the previous chapter, especially insofar as the introduction of functions of positive type makes a critical correspondence with the theory of unitary representations.

Another key element of the discussion is the definition of the Fourier transform in this abstract setting. Extending the notion of the real Fourier transform, we shall here associate with every suitable complex-valued function f on G a complex-valued transform $\hat{f}$ on $\hat{G}$. Moreover, we shall see that the functions f and $\hat{f}$ satisfy a generalized form of the Fourier inversion formula.

The locally compact abelian groups of most importance to us will ultimately be the additive and multiplicative groups associated with a local field F, which in characteristic zero must be $\mathbf{R}$, $\mathbf{C}$, or a finite extension of the p-adics $\mathbf{Q}_p$. In this context, the Fourier transform and the Fourier inversion formula bear heavily on Tate's thesis. To be more precise, the local zeta functions $Z(f,\chi,s)$ of Tate are defined, for $s\in\mathbf{C}$, with respect to an appropriate function f on a local field F and a character χ on F^*. The functional equation then relates $Z(f,\chi,s)$ to $Z(\hat{f},\overline{\chi},1-s)$, where $\overline{\chi}$ is the conjugate of the character χ. Hence this material is doubly critical to the sequel.

3.1 The Pontryagin Dual

Let G be an arbitrary group. If X is any subset of G, for $n\in\mathbf{N}$ define $X^{(n)}\subseteq G$ as follows:

$$X^{(n)} = \left\{ \prod_{j=1}^{n} x_j : x_j \in X, j = 1,\ldots,n \right\} .$$

Thus we explicitly distinguish between $X^{(n)}$ and the n-fold Cartesian product of X with itself.

Assume now that G is an abelian topological group, written multiplicatively. Define $\hat{G}$, the (multiplicative) *group of continuous complex characters of* G, to be the set of all continuous homomorphisms $G \rightarrow S^1$, where as usual, S^1 denotes the group of complex numbers of absolute value 1. $\hat{G}$ is also called the *Pontryagin dual* of G. Let K be a compact subset of G, and let V be a neighborhood of the identity in S^1. Then define the subset $W(K, V)$ of $\hat{G}$ by the formula

$$W(K,V) = \{\chi \in \hat{G} : \chi(K) \subseteq V\} .$$

The sets $W(K, V)$ constitute a neighborhood base for the trivial character and hence determine a topology on $\hat{G}$, called the *compact-open topology*. If G is discrete (in which case every compact set is finite), this topology evidently coincides with the topology of pointwise convergence.

We next define some key subsets in S^1. Recall that S^1 has universal cover given by the exponential map

$$\varphi : \mathbf{R} \rightarrow S^1$$
$$x \mapsto e^{2\pi i x}$$

which is in fact a continuous homomorphism with kernel $\mathbf{Z}$. Let ε be a real number such that $0 < \varepsilon \leq 1$. Define $N(\varepsilon) \subseteq S^1$ by

$$N(\varepsilon) = \varphi\left(\left(-\frac{\varepsilon}{3}, +\frac{\varepsilon}{3}\right)\right) .$$

Thus, $N(\varepsilon)$ is the image under φ of a symmetric open neighborhood of $0 \in \mathbf{R}$.

The key to the analysis of the compact-open topology on $\hat{G}$ is the following technical lemma.

3-1 LEMMA. *Let m be a positive integer and suppose that $x \in \mathbf{C}$ is such that $x, x^2, \ldots, x^m$ lie in $N(1)$. Then $x \in N(1/m)$. Consequently, if U is a subset of G containing the identity and $\chi : G \rightarrow S^1$ is a group homomorphism (not necessarily continuous) such that $\chi(U^{(m)}) \subseteq N(1)$, then $\chi(U) \subseteq N(1/m)$.*

PROOF. Let r be an arbitrary positive integer and suppose that x^r lies in $N(1)$. Then clearly there exists $y \in N(1/r)$ such that $x^r = y^r$, whence the quotient x/y is a

complex rth root of unity. Thus $x \in N(1/r)\varphi(q/r)$ for some integer q such that $0 \le q < r$. We shall now make a crucial observation about sets of the form $N(1/r)\varphi(q/r)$ that in passing explains the factor of one-third in the definition of $N(\varepsilon)$: for all positive integers r we have the implication

$$N(\frac{1}{r}) \cap N(\frac{1}{r+1})\varphi(\frac{q}{r+1}) \neq \varnothing \Rightarrow q = 0 \ .$$

The point is that

$$N(\frac{1}{r}) = \{\exp(\frac{2\pi it}{3}) : t \in (-\frac{1}{r}, +\frac{1}{r})\}$$

while

$$N(\frac{1}{r+1}) \cdot \varphi(\frac{q}{r+1}) = \{\exp(\frac{2\pi it}{3}) : t \in (\frac{3q-1}{r+1}, \frac{3q+1}{r+1})\} \ .$$

Hence the intervals indicated for the parameter t can have no intersection unless $1/r > (3q-1)/(r+1)$, which is to say that $2r+1 > 3qr$, an inequality that cannot hold unless $q=0$.

Suppose now that $x \in N(1/r)$ and $x^{r+1} \in N(1)$. Then $x \in N(1/(r+1))$ modulo an $(r+1)$th root of unity, and therefore by the observation of the last paragraph, in fact $x \in N(1/(r+1))$. Thus it follows by induction that if $x, x^2, \ldots, x^m$ lie in $N(1)$, then x lies in $N(1/m)$, as claimed.

The second statement follows immediately: Let $g \in U \subseteq G$, and suppose that U contains the identity. Then clearly $g, g^2, \ldots, g^m \in U^{(m)}$. Hence if $\chi(U^{(m)}) \subseteq N(1)$, $\chi(g)$ satisfies the hypotheses of the first part of the lemma. Thus $\chi(g) \in N(1/m)$ and $\chi(U) \subseteq N(1/m)$, as claimed. ❑

3-2 PROPOSITION. *Let G be an abelian topological group. Then the following assertions hold:*

(i) *A group homomorphism $\chi: G \to S^1$ is continuous, and hence a character of G, if and only if $\chi^{-1}(N(1))$ is a neighborhood of the identity in G.*

(ii) *The family $\{W(K, N(1))\}_K$ (indexed over all compact subsets of G) is a neighborhood base of the trivial character for the compact-open topology of $\hat{G}$.*

(iii) *If G is discrete, then $\hat{G}$ is compact.*

(iv) *If G is compact, then $\hat{G}$ is discrete.*

(v) *If G is locally compact, then $\hat{G}$ is likewise locally compact.*

PROOF. (i) Suppose that indeed there exists an open neighborhood U of the identity of G that maps into $N(1)$ via χ. Then since multiplication in G is continuous, for any positive integer m there exists an open neighborhood V of the identity in G such that $V^{(m)}$ is contained in U. Thus according to the previous lemma, $V^{(m)} \subseteq N(1/m)$, and χ is continuous.

(ii) We need to show that for every compact subset K_1 of G and for every positive m, there exists a compact subset K of G such that

$$W(K, N(1)) \subseteq W(K_1, N(1/m)) \ .$$

Let $K = K_1^{(m)}$, which is the continuous image of the compact set K^m (direct product), hence itself compact. If $\chi \in W(K,N(1))$, then by construction, for all $x \in K_1$, we have that $\chi(x), \chi(x)^2, \ldots, \chi(x)^m \in N(1)$. It follows now from the lemma that $\chi(x) \in N(1/m)$, whence $\chi \in W(K_1,N(1/m))$, as claimed.

(iii) If G is discrete, then $\hat{G} = \text{Hom}(G,S^1)$, the set of all algebra homomorphisms from G to the circle group. Moreover, as noted above, the compact-open topology on $\hat{G}$ is precisely the topology of pointwise convergence. But with respect to the latter topology, $\text{Hom}(G,S^1)$ is evidently a closed subset of the space of all maps from G to S^1, which is itself compact. Hence $\hat{G}$ is compact.

(iv) Given any character χ, $\chi(G)$ is a subgroup of S^1 and hence not contained in any set of the form $N(\varepsilon)$, $0 < \varepsilon \leq 1$. Thus if G is compact, then $W(G,N(1))$ can contain only the trivial character, which therefore constitutes an open subset of $\hat{G}$. It follows at once that $\hat{G}$ is discrete.

(v) To show that $\hat{G}$ is locally compact, we shall show that if K is any fixed compact neighborhood of the identity of G, then

$$W = W(K, \overline{N(1/4)})$$

is a compact neighborhood of the identity in $\hat{G}$. (Here the bar denotes closure.) By part (ii), this suffices, since $\{W(K,N(1))\}$ for K compact is a neighborhood base at the identity.

Let G_0 denote the discrete topological group having the same group structure as G. Note that only finite subsets of G_0 are compact. From parts (iii) and (iv) we know that $\hat{G}_0$, is just $\text{Hom}(G,S^1)$ with the topology of pointwise convergence and that $\hat{G}_0$ is compact. Define W_0 by

$$W_0 = \{\chi \in \hat{G}_0 : \chi(K) \subseteq \overline{N(1/4)}\} \ .$$

Now clearly W_0 is closed in $\hat{G}_0$, and is therefore itself compact. Moreover, $W_0 \subseteq W$ by part (i), and certainly $W \subseteq W_0$, since $\hat{G}_0$ ignores continuity. Hence

$$W = W_0$$

and if τ_0 denotes the topology induced on W by $\hat{G}_0$, and τ denotes the topology on W induced by $\hat{G}$, it suffices to show that τ_0 is finer than τ; for then the compactness of W with respect to τ_0 will imply its compactness with respect to τ, as required. (In fact, the two topologies are then equal, since τ, the compact-open topology, is clearly finer than τ_0, the topology of pointwise convergence.) Let K_1 be a compact subset of G and let m be a positive integer. For each $\chi \in W$, consider the subset

$$W(\chi) = (\chi W(K_1, N(1/m))) \cap W \ .$$

We shall show that each $W(\chi)$ is an open neighborhood of χ with respect to τ_0, whence τ has a neighborhood base at χ contained in τ_0.

Let V be an open neighborhood of the identity in G such that $V^{(2m)} \subseteq K$. Since K_1 is compact, there exists a finite set F such that $F \cdot V \supseteq K_1$. Define a subset $W_0(\chi)$ of W as follows:

$$W_0(\chi) = (\chi W_0(F, N(1/(2m)))) \cap W$$

where $W_0(F, N(1/(2m)))$ denotes the set of characters on G_0 that map F into $N(1/(2m))$. We claim that $W_0(\chi)$ is a τ_0-neighborhood of χ contained in $W(\chi)$, and this will complete the proof. Since $W_0(F, N(1/(2m)))$ is clearly open in $\hat{G}_0$, only the inclusion $W_0(\chi) \subseteq W(\chi)$ needs verification.

Let $\mu \in W_0(\chi)$. Then by construction, $\mu = \chi\mu_0 \in W$ for some $\mu_0 \in \hat{G}_0$ such that $\mu_0(F) \subseteq N(1/(2m))$. Since clearly $\mu_0 = \chi^{-1}\mu \in W^{(2)}$, it follows that

$$\mu_0(K) \subseteq N(1/2) \subseteq N(1) \ .$$

From this we may draw two conclusions:

(a) The character μ_0 is continuous [according to part (i)].

(b) By the assumption that $V^{(2m)} \subseteq K$ and by the preceding lemma, we have that $\mu_0(V) \subseteq N(1/(2m))$ and hence the following chain of inclusions:

$$\mu_0(K_1) \subseteq \mu_0(F) \cdot \mu_0(V) \subseteq N(1/(2m)) \cdot N(1/(2m)) = N(1/m) \ .$$

The upshot is that μ_0 in fact lies in $W(K_1, N(1/m))$, and therefore μ lies in $W(\chi)$. Thus $W_0(\chi)$ is indeed contained in $W(\chi)$, as required. ❑

3.2 Functions of Positive Type

In order to motivate the principal definition of this discussion, we begin with an elementary observation about unitary representations.

Let ρ be a representation of the topological group G (not necessarily locally compact or abelian) in the space of unitary operators of a Hilbert space H. For our current purposes, for any $s \in G$ it will be convenient to write $\rho(s)$ rather than ρ_s for the associated operator. Fix $x \in H$. We may now define a complex-valued function φ on G as follows:

$$\varphi(s) = \langle \rho(s)(x) | x \rangle \ .$$

Let $s_1,\ldots,s_n$ be any family of elements in G and consider the complex $n \times n$ matrix

$$A = (\varphi(s_j^{-1} s_i)) \ .$$

We claim that A is both Hermitian and positive semidefinite. The first point is trivial: since each $\rho(s)$ is unitary,

$$\langle \rho(s_j^{-1} s_i)(x) | x \rangle = \langle \rho(s_i)(x) | \rho(s_j)(x) \rangle = \overline{\langle \rho(s_j)(x) | \rho(s_i)(x) \rangle} = \overline{\langle \rho(s_i^{-1} s_j)(x) | x \rangle} \ .$$

For the second, consider any complex vector $z = (z_i) \in \mathbf{C}^n$. Then we compute

$$\begin{aligned} \langle Az | z \rangle &= \sum_{i,j=1}^{n} \varphi(s_j^{-1} s_i) z_j \bar{z}_i \\ &= \sum_{i,j=1}^{n} \langle \rho(s_i)(x) | \rho(s_j)(x) \rangle z_j \bar{z}_i \\ &= \langle \sum_{j=1}^{n} \rho(s_j)(z_j x) | \sum_{i=1}^{n} \rho(s_i)(z_i x) \rangle \\ &= |\sum_{i=1}^{n} \rho(s_i)(z_i x)|^2 \geq 0 \ . \end{aligned}$$

This analysis will lead shortly to a key definition in which the preceding inequality appears in continuous form.

Assume now that G is a locally compact group with (left) Haar measure ds. Let $\mathscr{C}_c(G)$ denote the set of complex-valued continuous functions on G with compact support. Recall that for every p, $1 \leq p \leq \infty$, $\mathscr{C}_c(G)$ is contained in the Banach space $L^p(G)$ and is hence subject to the L^p-norm and associated topology defined by

$$\|f\|_p = \left\{ \int_X |f|^p \, dx \right\}^{1/p}$$

for finite p, with $\|f\|_\infty$ defined to be the essential supremum of $|f|$. [See Appendix A, Section A.4. Note that $L^\infty(G)$ consists of functions in $L(G)$ with finite essential supremum.] In fact, for all p, $\mathscr{C}_c(G)$ is dense in $L^p(G)$.

DEFINITION. Let G be a locally compact topological group. Then a Haar-measurable function $\varphi: G \to \mathbf{C}$ in $L^\infty(G)$ is said to be of *positive type* (or *positive definite*) if for any $f \in \mathscr{C}_c(G)$ the following inequality holds:

$$\iint \varphi(s^{-1}t) f(s) \, ds \, \overline{f(t)} \, dt \geq 0 \quad .$$

Both integrals are implicitly over the full group G.

Note that the integrand is Haar measurable on $G \times G$ by Exercise 1 below, and so Fubini's theorem applies to show that this double integral is in fact defined. (Every locally compact group is the disjoint union of σ-compact spaces; see Section A.4 of the Appendices.) Moreover, if the support of f is contained in the compact subset $K \subseteq G$, then the integrand has support contained in the compact subset $K \times K$ of $G \times G$. Since φ is in $L^\infty(G)$, it is bounded by $\|\varphi\|_\infty$, the essential supremum of φ, except on a set of measure zero. Thus the integral is itself bounded as follows:

$$\left| \iint \varphi(s^{-1}t) f(s) \, ds \, \overline{f(t)} \, dt \right| \leq \|\varphi\|_\infty (\sup |f| \cdot \mu(K))^2 \quad . \tag{3.1}$$

Here $\mu(K)$ is the (necessarily finite) Haar measure of K.

To establish some fundamental properties of functions of positive type, we make two connections: first with Hilbert spaces and second with unitary representations.

If φ is a function of positive type, we can define a positive sesquilinear (and hence conjugate symmetric) form on $\mathscr{C}_c(G)$ by the formula

$$\langle f_1 | f_2 \rangle_\varphi = \iint \varphi(s^{-1}t) f_1(s) \, ds \, \overline{f_2(t)} \, dt \quad .$$

Analysis similar to that above shows that this integral is defined and finite for all f_1 and f_2 in $\mathscr{C}_c(G)$. Put

$$W_\varphi = \{ f \in \mathscr{C}_c(G) : \langle f | f \rangle_\varphi = 0 \} \quad .$$

It follows from the Cauchy-Schwarz inequality (the proof of which does *not* require positive definiteness) that W_φ is a subspace of $\mathscr{C}_c(G)$ and that W_φ con-

sists of those functions that are degenerate with respect to φ. We may thus form the quotient space $\mathscr{C}_c(G)/W_\varphi$, on which, by construction, $\langle\,|\,\rangle_\varphi$ is a positive definite Hermitian form. Let V_φ denote the completion of this quotient, to which the form $\langle\,|\,\rangle_\varphi$ extends by continuity. Accordingly, V_φ acquires the structure of a Hilbert space.

Let f be any function on G and recall that for any $s \in G$, we define $L_s f$ on G as follows:

$$L_s f(t) = f(s^{-1}t) \ .$$

In the particular case that $f \in \mathscr{C}_c(G)$, then also $L_s f \in \mathscr{C}_c(G)$ by the continuity of the group laws and one checks easily that the mapping

$$\begin{aligned} G &\to \mathrm{End}(\mathscr{C}_c(G)) \\ s &\mapsto L_s \end{aligned}$$

is an abstract representation of G. Moreover, if φ is a function of positive type on G, and f is again in $\mathscr{C}_c(G)$, then

$$\begin{aligned} \langle L_s f | L_s f \rangle_\varphi &= \iint \varphi(t^{-1}u) f(s^{-1}t)\, dt\, \overline{f(s^{-1}u)}\, du \\ &= \iint \varphi((s^{-1}t)^{-1}(s^{-1}u)) f(s^{-1}t)\, dt\, \overline{f(s^{-1}u)}\, du \\ &= \iint \varphi(t^{-1}u) f(t)\, dt\, \overline{f(u)}\, du \\ &= \langle f | f \rangle_\varphi \ . \end{aligned}$$

This shows that L induces at least an abstract unitary representation of G on the Hilbert space V_φ. To see that L is moreover a topological representation, it suffices by Corollary 2-2 to show that for every $f \in \mathscr{C}_c(G)$ the mapping

$$\begin{aligned} G &\to \mathscr{C}_c(G) \\ s &\mapsto L_s f \end{aligned}$$

is continuous, which is to say that if $s_\alpha \to s$ in G, then $L_{s_\alpha} f \to L_s f$ in $\mathscr{C}_c(G)$ with respect to the φ-norm. According to inequality 3.1, this will be the case, provided that the obvious pointwise convergence

$$f(s_\alpha^{-1}t) \to f(s^{-1}t)$$

for $t \in G$ is uniform. But clearly $s_\alpha^{-1}t \to s^{-1}t$ uniformly in G, whence the required uniform convergence follows from Exercise 2 below. We summarize this discussion in the following proposition:

3-3 PROPOSITION. *Let G be a locally compact group and let φ be a function of positive type on G. Then the mapping $s \mapsto L_s$ induces a unitary representation of G on the associated Hilbert space V_φ.* ❑

Further properties of functions of bounded type depend on a more detailed examination of the representation above.

Definition of Convolution and the Representation of Bounded Functions of Positive Type

The representation described above of G on V_φ allows us to represent a bounded function φ of positive type in the following sense: there exists a function $x_\varphi \in V_\varphi$ such that

$$\varphi(s) = \langle x_\varphi | L_s x_\varphi \rangle_\varphi$$

almost everywhere for $s \in G$. To develop this result, we need first to recall the notion of convolution of functions on G.

Let f and g be complex-valued Borel functions on a locally compact topological group G. Then their *convolution* $f*g$ is defined by

$$f*g(t) = \int g(s^{-1}t) f(s)\, ds = \int g(s^{-1}) f(ts)\, ds$$

provided that this integral, taken over the full group with respect to the (left) Haar measure ds, exists. We shall make a more systematic study of the key properties of convolution in the following section. In connection with our current study of functions of positive type, we are interested in the special case $f*\varphi$ where $f \in \mathscr{C}_c(G)$, $\varphi \in L^\infty(G)$. Under these conditions, clearly $f*\varphi$ exists. Moreover, if $t_\alpha \to t$ in G, then

$$\int \varphi(s^{-1})(f(ts) - f(t_\alpha s))\, ds \to 0$$

and it follows that $f*\varphi$ is continuous.

3-4 PROPOSITION. *Let φ be a function of positive type on G. Then there exists an element $x_\varphi \in V_\varphi$ such that*

$$\varphi(s) = \langle x_\varphi | L_s x_\varphi \rangle_\varphi$$

almost everywhere for $s \in G$.

PROOF. Let $\{\alpha\}$ be an index set for the collection of open neighborhoods V_α of the identity of G. Since G is Hausdorff, clearly $\{e\}=\bigcap_\alpha V_\alpha$, and if we write $\alpha \le \beta$ whenever $V_\beta \subseteq V_\alpha$, then $\{\alpha\}$ is a directed set. It follows from Urysohn's lemma for locally compact spaces that for index α, we can construct a continuous function $g_\alpha : G \to \mathbf{R}_+$ such that

(i) the support of g_α is a compact subset of V_α;

(ii) each g_α satisfies the equality

$$\int_G g_\alpha(s)ds = 1 \ .$$

This simultaneously defines a net $\{g_\alpha(s)\,ds\}$ of positive linear functionals on $\mathscr{C}_c(G)$:

$$f \mapsto \int_G f(s) g_\alpha(s)ds \ .$$

Evidently these converge weakly to the Dirac measure δ_e, which is nothing more than evaluation at the identity e; that is,

$$\delta_e(f) = f(e) \ .$$

Let $f \in \mathscr{C}_c(G)$, and let g_α be as above. Consider the integral

$$\iint \varphi(s^{-1}t) f(s)\,ds\, g_\alpha(t)\,dt = \int f * \varphi(t) \cdot g_\alpha(t)\,dt$$

which exists, since $f*\varphi$ is continuous and g has compact support. We may now define a linear form Φ on V_φ that on $\mathscr{C}_c(G)$ is given by

$$\Phi(f) = \lim_\alpha \langle f \mid g_\alpha \rangle_\varphi = \lim_\alpha \iint \varphi(s^{-1}t) f(s)\,ds\, g_\alpha(t)\,dt = \lim_\alpha \int f * \varphi(t) \cdot g_\alpha(t)\,dt \ .$$

To see that this limit exists and that in fact

$$\Phi(f) = f * \varphi(e) = \int \varphi(s^{-1}) f(s) ds$$

it suffices to note that in order to compute $\Phi(f)$ we may replace the factor $f*\varphi$ in the integrand by the product $(f*\varphi)\cdot h$, where $h \in \mathscr{C}_c(G)$ is a fixed function that takes the value 1 in a neighborhood of e that contains the eventual support of g_α. Hence $(f*\varphi)\cdot h$ lies in $\mathscr{C}_c(G)$, and the previous equality is nothing more

than the weak convergence of $g_\alpha(s)ds$ to δ_e. Now since V_φ is self-dual, there exists an element $x_\varphi \in V_\varphi$ such that

$$\Phi(\xi) = \langle \xi | x_\varphi \rangle_\varphi$$

for all $\xi \in V_\varphi$; this is to say that the g_α converge weakly in V_φ to x_φ.

We shall see next how x_φ behaves under the continuous group action from G defined by $s \mapsto L_s$. First we compute

$$\begin{aligned}\langle \xi | L_s x_\varphi \rangle_\varphi &= \lim_\alpha \langle \xi | L_s g_\alpha \rangle_\varphi \\ &= \lim_\alpha \iint \varphi(t^{-1}u)\xi(t)\,dt\, g_\alpha(s^{-1}u)\,du \\ &= \int \varphi(t^{-1}s)\,\xi(t)\,dt \quad .\end{aligned}$$

Next we compute the inner product in reverse order:

$$\begin{aligned}\langle L_s x_\varphi | \xi \rangle_\varphi &= \lim_\alpha \langle L_s g_\alpha | \xi \rangle_\varphi \\ &= \lim_\alpha \iint \varphi(t^{-1}u) g_\alpha(s^{-1}t)\,dt\,\overline{\xi(u)}\,du \\ &= \int \varphi(s^{-1}u)\,\overline{\xi(u)}\,du \quad .\end{aligned}$$

By the conjugate symmetry of the Hermitian form $\langle\,|\,\rangle_\varphi$, it now follows at once from the two previous equations that

$$\langle \xi | L_s x_\varphi \rangle_\varphi = \int \varphi(t^{-1}s)\,\xi(t)\,dt = \int \overline{\varphi(s^{-1}t)}\,\xi(t)\,dt \quad . \tag{3.2}$$

In the special case that $s=e$, we have, in particular, that

$$\langle \xi | x_\varphi \rangle_\varphi = \int \overline{\varphi(s)}\,\xi(s)ds \quad . \tag{3.3}$$

From Eq. 3.2 we deduce immediately that for arbitrary $h \in \mathscr{C}_c(G)$,

$$\begin{aligned}\langle \xi | h \rangle_\varphi &= \iint \varphi(s^{-1}t)\,\xi(s)\,ds\,\overline{h(t)}\,dt \\ &= \int \langle \xi | L_t x_\varphi \rangle_\varphi \overline{h(t)}dt\end{aligned}$$

and by (strong) continuity this equality clearly extends to all of V_φ. This shows that if ξ is orthogonal to the CG-submodule of V_φ generated by x_φ, then ξ is zero in V_φ. Thus V_φ is in fact generated as a CG-module by x_φ. In the special

case $\xi = x_\varphi$, the previous equation together with Eq. 3.3 shows that for all $\psi \in V_\varphi$,

$$\int \varphi(s)\overline{\psi(s)}ds = \langle x_\varphi | \psi \rangle_\varphi = \int \langle x_\varphi | L_s x_\varphi \rangle_\varphi \overline{\psi(s)}ds$$

whence

$$\varphi(s) = \langle x_\varphi | L_s x_\varphi \rangle_\varphi$$

almost everywhere, as required. ❑

3-5 COROLLARY. *Let φ be as above. Then φ is equal to a continuous function of positive type almost everywhere. If, moreover, φ is itself continuous, then we have further that:*

(i) $\varphi(e) \geq 0$.

(ii) $\varphi(e) = \sup|\varphi(s)|$, *where s ranges over G.*

(iii) $\varphi(s^{-1}) = \overline{\varphi(s)}$ *for all $s \in G$.*

PROOF. The main statement is obvious from the representation of φ given in the proposition: the inner product is continuous by the polarization identity from linear algebra. For assertion (i), note that

$$\varphi(e) = \langle x_\varphi | L_e x_\varphi \rangle_\varphi = \langle x_\varphi | x_\varphi \rangle_\varphi \geq 0 \ .$$

Next, (ii) follows from the Cauchy-Schwarz inequality:

$$\varphi(s)^2 = \langle x_\varphi | L_s x_\varphi \rangle_\varphi^2 \leq \langle x_\varphi | x_\varphi \rangle_\varphi \langle L_s x_\varphi | L_s x_\varphi \rangle_\varphi = \langle x_\varphi | x_\varphi \rangle_\varphi^2 = \varphi(e)^2 \ .$$

The key, of course, is that L_s is unitary. Finally, (iii) is again an easy exercise in unitary operators:

$$\varphi(s^{-1}) = \langle x_\varphi | L_{s^{-1}} x_\varphi \rangle_\varphi = \langle L_s x_\varphi | x_\varphi \rangle_\varphi = \overline{\langle x_\varphi | L_s x_\varphi \rangle_\varphi} = \overline{\varphi(s)} \ .$$ ❑

Elementary Functions

The functions of positive type that are continuous on G and bounded by 1 in the L^∞-norm constitute an important subset of $L^\infty(G)$ denoted $\mathscr{P}(G)$; that is,

$$\mathscr{P}(G) = \{\varphi \in \mathscr{C}(G) \cap L^\infty(G) : \varphi \text{ is a positive type and } \|\varphi\|_\infty \leq 1\} \ .$$

Note that by the corollary above, in this case the condition $\|\varphi\|_\infty \leq 1$ amounts to nothing more than $\varphi(e) \leq 1$.

A related collection of L^∞-functions, denoted $\mathscr{E}(G)$, is defined as follows. A function φ lies in $\mathscr{E}(G)$ if it is the zero map or if it satisfies the following three conditions:

(i) φ is continuous and of positive type.

(ii) $\varphi(e)=1$.

(iii) For every decomposition $\varphi=\varphi_1+\varphi_2$ into the sum of two functions φ_1, φ_2 both lying in $\mathscr{P}(G)$, there exist positive real constants λ_1 and λ_2 such that

$$\varphi_1 = \lambda_1 \varphi, \ \ \varphi_2 = \lambda_2 \varphi \ \ (\text{whence } \lambda_1 + \lambda_2 = 1) \ .$$

The nonzero elements of $\mathscr{E}(G)$ are called *elementary functions.* Note that condition (iii) asserts that elements of $\mathscr{E}(G)$ are in fact extreme points of $\mathscr{P}(G)$.

3-6 LEMMA. $\mathscr{P}(G)$ and $\mathscr{E}(G)$ *have the following properties:*

(i) $\mathscr{P}(G)$ *is a convex, bounded subset of* $L^\infty(G)$. *It is, moreover, weakly closed and therefore weakly compact as a subset of* $L^1(G)^*$.

(ii) *Any convex, closed subset of* $\mathscr{P}(G)$ *containing its extreme points is all of* $\mathscr{P}(G)$.

(iii) *The extreme points of* $\mathscr{P}(G)$ *consist precisely of the points of* $\mathscr{E}(G)$.

PROOF. (i) $\mathscr{P}(G)$ is obviously convex and bounded. Now identify elements of $\mathscr{P}(G)$ with elements of $L^1(G)^*$ in accordance with the usual duality theory for L^p-spaces (see Section A.4 of Appendix A). Recall in particular that the infinity norm of an element in $L^\infty(G)$ is identical to the norm of the corresponding functional between the Banach spaces $L^1(G)$ and $\mathbf{C}$. To say that a sequence φ_n of functions in $\mathscr{P}(G)$ is weakly convergent to some $\varphi \in L^\infty(G)$ is to say that for all $f \in L^1(G)$ we have

$$\int f\varphi_n \, ds \to \int f\varphi ds \ .$$

It follows at once from this that $\|\varphi\|_\infty \leq 1$ and that

$$\iint \varphi_n(s^{-1}t) f(s) ds \overline{f(t)} dt \to \iint \varphi(s^{-1}t) f(s) ds \overline{f(t)} dt$$

whence φ is also of positive type and therefore continuous by the previous corollary. [More precisely, φ represents the equivalence class of a continuous function in $L^\infty(G)$]. Thus as a subset of $L^1(X)^*$, $\mathscr{P}(G)$ corresponds to a closed

subset of the unit ball, which is therefore compact under the weak-star topology by Alaoglu's theorem.

(ii) This is a special case of the Krein-Milman theorem.

(iii) The only point to check is that a nonzero extreme point $\varphi \in \mathscr{P}(G)$ satisfies $\varphi(e)=1$. But if $\varphi(e)<1$, then also

$$\frac{1}{\varphi(e)}\varphi$$

lies in $\mathscr{P}(G)$, and φ is not extreme. ❑

This brings us to a striking and exquisite theorem that connects the elementary functions with irreducible representations.

3-7 THEOREM. *Let φ be a continuous function of positive type on G such that $\varphi(e)=1$. Then $\varphi \in \mathscr{E}(G)$ if and only if the unitary representation $s \mapsto L_s$ of G in V_φ is irreducible; that is, V_φ itself and the zero subspace are the only closed subspaces of V_φ that are invariant under each of the transformations L_s, for $s \in G$.*

PROOF. $\Rightarrow$) Assume that φ is an elementary function. Let W be a closed G-invariant subspace of V_φ, with orthogonal complement $W^\perp$. Let pr_W denote the orthogonal projection map into W. Then since each operator L_s is unitary, we have the following commutative diagram:

$$\begin{array}{ccc} W \oplus W^\perp & \xrightarrow{\mathrm{pr}_W} & W^\perp \\ L_s \downarrow & & \downarrow L_s \\ W \oplus W^\perp & \xrightarrow{\mathrm{pr}_W} & W^\perp \end{array}$$

Thus it suffices to show that if A is any orthogonal projection operator that commutes with each L_s, then A is either the zero map or the identity map on V_φ. Since in general we have $\langle Ax|y\rangle_\varphi = \langle Ax|Ay\rangle_\varphi$ for any projection, it follows that for all $s \in G$,

$$\begin{aligned} \varphi(s) &= \langle x_\varphi | L_s x_\varphi \rangle_\varphi \\ &= \langle Ax_\varphi | L_s x_\varphi \rangle_\varphi + \langle x_\varphi - Ax_\varphi | L_s x_\varphi \rangle_\varphi \\ &= \langle Ax_\varphi | L_s A x_\varphi \rangle_\varphi + \langle x_\varphi - Ax_\varphi | L_s (x_\varphi - Ax_\varphi) \rangle_\varphi \ . \end{aligned}$$

This expresses φ as the sum of two functions that, by Exercise 4, are of positive type. Hence under the assumption that φ is extreme,

$$\langle Ax_\varphi | L_s x_\varphi \rangle_\varphi = \lambda \langle x_\varphi | L_s x_\varphi \rangle_\varphi$$

for all $s \in G$, and it follows that $A = \lambda \cdot 1_{V_\varphi}$, because as we observed in the proof of the representation theorem for functions of positive type, x_φ generates V_φ as a $\mathbf{C}G$-module. But since A is idempotent, this forces λ to be 0 or 1, as required.

$\Leftarrow$) Suppose that the given representation of G in V_φ is indeed irreducible and that $\varphi = \varphi_1 + \varphi_2$ is a decomposition of φ into the sum of two functions from $\mathscr{P}(G)$. Then for each $f \in \mathscr{C}_c(G)$, one observes easily that

$$\langle f | f \rangle_{\varphi_1} \leq \langle f | f \rangle_\varphi \ .$$

From this it follows that any element of $\mathscr{C}_c(G)$ that is degenerate with respect to $\langle \, | \, \rangle_\varphi$ is also degenerate with respect to $\langle \, | \, \rangle_{\varphi_1}$. Thus φ_1 likewise defines a Hermitian form on V_φ, and accordingly there exists a continuous positive definite endomorphism A of V_φ such that

$$\langle A\xi | \psi \rangle_\varphi = \langle \xi | \psi \rangle_{\varphi_1}$$

for all $\xi, \psi \in V_\varphi$. Thus, in particular,

$$\langle Ax_\varphi | L_s x_\varphi \rangle_\varphi = \langle x_\varphi | L_s x_\varphi \rangle_{\varphi_1}$$

for all $s \in G$. But also

$$\langle x_\varphi | L_s x_\varphi \rangle_{\varphi_1} = \varphi_1(s) \ .$$

The point here is that in the proof of Proposition 3-4, the convergence of the net $\{g_\alpha\}$ to x_φ with respect to the $\langle \, | \, \rangle_\varphi$-norm will also hold with respect to the $\langle \, | \, \rangle_{\varphi_1}$-norm by virtue of the last-stated inequality. Thus φ_1 is likewise represented by x_φ in the sense above. The upshot is that

$$\langle Ax_\varphi | L_s x_\varphi \rangle_\varphi = \varphi_1(s) \ .$$

We claim now that A commutes with each L_s. Granting this, Schur's lemma for unitary representations (Theorem 2-26) implies that A is a scalar multiple λ of the identity map on V_φ, and therefore

$$\varphi_1(s) = \langle \lambda x_\varphi | L_s x_\varphi \rangle_\varphi = \lambda \varphi(s)$$

showing that φ is indeed extreme.

Finally, to establish the claim we rely on the unitary nature of L_s and compute as follows:

$$\begin{aligned}\langle AL_s\varphi \mid \psi\rangle_\varphi &= \langle L_s\varphi \mid \psi\rangle_{\varphi_1} \\ &= \langle \varphi \mid L_{s^{-1}}\psi\rangle_{\varphi_1} \\ &= \langle A\varphi \mid L_{s^{-1}}\psi\rangle_\varphi \\ &= \langle L_sA\varphi \mid \psi\rangle_\varphi\end{aligned}$$

for all $s\in G$ and $\varphi, \psi\in\mathscr{C}_c(G)$. This completes the proof. ❑

We can now make an enlightening connection between functions of positive type and group characters. Here, at long last, we assume that G is abelian.

3-8 THEOREM. *Let G be a locally compact abelian topological group. Then the elementary functions of positive type on G are precisely the (continuous) characters of G.*

PROOF. Note first that a character χ on G is clearly a bounded function in $L^\infty(G)$. Moreover, by the following calculation it is of positive type:

$$\begin{aligned}\iint \chi(s^{-1}t)f(s)\,ds\,\overline{f(t)}\,dt &= \iint \overline{\chi(s)}\chi(t)f(s)\,ds\,\overline{f(t)}\,dt \\ &= \int \overline{\chi(s)}f(s)\,ds \cdot \int \chi(t)\,\overline{f(t)}\,dt \\ &= \left|\int \overline{\chi(s)}f(s)\,ds\right|^2\end{aligned}$$

for all $f\in\mathscr{C}_c(G)$. Since necessarily $\chi(e)=1$, in light of the previous theorem it suffices to show that given a continuous function φ of positive type on G such that $\varphi(e)=1$, the following conditions are equivalent:

(i) The representation of G in V_φ is irreducible.

(ii) φ is a character of G.

One implication is straightforward; the other depends on spectral theory.

(ii)$\Rightarrow$(i) Suppose that φ is a character of G and consider a function $f\in\mathscr{C}_c(G)$. Then as above,

$$\begin{aligned}\langle f \mid f\rangle_\varphi &= \iint \varphi(s^{-1}t)f(s)\,ds\,\overline{f(t)}\,dt \\ &= \left|\int \overline{\varphi(s)}f(s)\,ds\right|^2 .\end{aligned}$$

The point is that the subspace of $\mathscr{C}_c(G)$ consisting of functions degenerate with respect to the form $\langle\,|\,\rangle_\varphi$ has codimension 1, and hence V_φ is a 1-dimensional and therefore irreducible representation of G.

(i)$\Rightarrow$(ii) Assume now that the representation of G via φ in V_φ is irreducible. Then as a consequence of Schur's lemma (specifically, Theorem 2-27), the representation $s \mapsto L_s$ is one-dimensional, whence for all $\xi \in V_\varphi$,

$$L_s(\xi) = \lambda(s)\xi$$

where $\lambda(s)$ evidently depends continuously on s. Moreover, it is clear from the preceding equation that indeed λ is a character of G. Finally,

$$\varphi(s) = \langle x_\varphi | L_s x_\varphi \rangle_\varphi = \overline{\lambda(s)}\langle x_\varphi | x_\varphi \rangle_\varphi = \overline{\lambda(s)}\,\varphi(e) = \overline{\lambda(s)}$$

whence φ is likewise a character, as claimed. ❑

3.3 The Fourier Inversion Formula

The principal technical tool for establishing the Pontryagin duality theorem in the following section is the Fourier inversion formula. In this section we review the Fourier transform and prove this fundamental result. Throughout, G denotes a locally compact abelian group with bi-invariant Haar measure dx and continuous complex character group $\hat{G}$.

DEFINITION. Let $f \in L^1(G)$. Then we define $\hat{f}: \hat{G} \to \mathbf{C}$, the *Fourier transform* of f, by the formula

$$\hat{f}(\chi) = \int_G f(y)\overline{\chi}(y)\,dy$$

for $\chi \in \hat{G}$.

Note that this formula makes sense, since for all $y \in G$, $\chi(y)$ has norm 1. Hence if f is integrable, so is the product appearing in the integrand. Moreover, one verifies at once that $|\hat{f}(\chi)| \le \|f\|_1$ for $f \in L^1(G)$, $\chi \in \hat{G}$.

REMARK. In the special case that $G = \mathbf{R}$, the topological group of real numbers with respect to addition, we can identify each $t \in \mathbf{R}$ with the character

$$s \mapsto e^{ist}\ .$$

In this case the formula above reduces to

$$\hat{f}(t) = \int_{\mathbf{R}} f(s)e^{-ist}ds$$

which is of course the ordinary Fourier transform of a function defined on **R**. The point is that despite appearances, this should in fact be regarded as a function on $\hat{\mathbf{R}}$.

Let $V(G)$ denote the complex span of the continuous functions of positive type on G, and define

$$V^1(G) = V(G) \cap L^1(G) \ .$$

We can now state the principal result of this section. (See Exercises 13 and 14 below for direct proofs of this theorem and the duality theorem for G finite.)

3-9 THEOREM. (The Fourier Inversion Formula) *There exists a Haar measure $d\chi$ on $\hat{G}$ such that for all $f \in V^1(G)$,*

$$f(y) = \int_{\hat{G}} \hat{f}(\chi)\chi(y)\,d\chi \ .$$

Moreover, the Fourier transform $f \mapsto \hat{f}$ identifies $V^1(G)$ with $V^1(\hat{G})$.

The measure $d\chi$ of the theorem is called the *dual measure* of dx, the given Haar measure on G. To prove its existence, we must begin with some elementary properties of convolution.

3-10 PROPOSITION. *Let f and g be complex-valued Borel functions on the locally compact abelian group G. Then the following statements hold:*

(i) *If the convolution $f*g(x)$ exists for some $x \in G$, then so does $g*f(x)$, and in fact $g*f(x) = f*g(x)$.*

(ii) *If $f, g \in L^1(G)$, then $f*g(x)$ exists for almost all $x \in G$; moreover, $f*g \in L^1(G)$ and*

$$\|f*g\|_1 \leq \|f\|_1 \, \|g\|_1 \ .$$

(iii) *If $f, g, h \in L^1(G)$, then $(f*g)*h = f*(g*h)$.*

Thus, in particular, convolution is both associative and commutative on $L^1(G)$.

PROOF. (i) This follows by direct application of the translation-invariance of the Haar measure on G. We replace y by yx in the integrand that defines convolution to obtain

$$\begin{aligned} f*g(x) &= \int g(y^{-1}x)f(y)dy \\ &= \int g(y^{-1})f(yx)dy \\ &= g*f(x) \ . \end{aligned}$$

Note that the last step is justified by the elementary observation that for locally compact abelian groups, the Haar measure of a Borel subset E of G is equal to that of E^{-1}. (See Exercise 7 below.)

(ii) First consider the homeomorphism α from $G\times G$ to itself defined by

$$\alpha(x,y) = (yx,y) \ .$$

Observe that the inverse map sends (x,y) to $(y^{-1}x,y)$. Next consider an open subset $U\subseteq \mathbf{C}$. Then $\alpha(f^{-1}(U)\times G)$ is clearly a Borel subset of $G\times G$, and by construction, $(x,y)\in\alpha(f^{-1}(U)\times G)$ if and only if $y^{-1}x\in f^{-1}(U)$. This shows that the mapping

$$(x,y)\mapsto f(y^{-1}x)$$

is a Borel function on $G\times G$, and hence so is

$$(x,y)\mapsto f(y^{-1}x)g(y)$$

since the product of Borel functions is again a Borel function. (Here we may view g as a function on $G\times G$ in the obvious way.) Since both f and g are L^1-functions, we have

$$\iint |f(y^{-1}x)|\,dx\,|g(y)|\,dy < \infty$$

and therefore Fubini's theorem applies to yield

$$\iint |f(y^{-1}x)g(y)|\,dy\,dx = \|f\|_1 \|g\|_1 \ .$$

It follows that $|f|*|g|$ is an L^1-function and hence is finite almost everywhere; so, too, then for $f*g$. Finally, the inequality of norms is clear from the previous equation.

(iii) Associativity follows by a calculation that again depends on Fubini's theorem; the requisite hypotheses are guaranteed for almost all x by part (ii). To begin,

$$\begin{aligned} f*(g*h)(x) &= \int f(y^{-1}x)(g*h)(y)\,dy \\ &= \int f(y^{-1}x)\int g(z^{-1}y)h(z)\,dz\,dy \\ &= \iint f(y^{-1}x)g(z^{-1}y)h(z)\,dy\,dz \ . \end{aligned}$$

Now replace y by yz in the inner integral to obtain

$$\begin{aligned} f*(g*h)(x) &= \iint f(y^{-1}z^{-1}x)g(y)h(z)\,dy\,dz \\ &= \int f*g(z^{-1}x)\,h(z)\,dz \\ &= (f*g)*h(x) \ . \end{aligned}$$

This completes the proof. ❑

We may infer from the previous result that for G as above, $L^1(G)$ constitutes a Banach algebra with respect to convolution. One sees easily that if G is discrete, then $L^1(G)$ has a unit (the characteristic function of the group identity). The converse also holds. The Banach algebra structure of $L^1(G)$ allows us to make an explicit connection between the Fourier transform and the Gelfand transform.

3-11 PROPOSITION. *Let B denote the Banach algebra $L^1(G)$, and as usual let $\hat{B} = Hom_{\mathbf{C}}(B,\mathbf{C})^*$ denote the space of (nonzero) complex characters of B. For any given character χ of G and function $f \in L^1(G)$, define*

$$\hat{v}_\chi(f) = \hat{f}(\chi) = \int f(y)\overline{\chi(y)}\,dy \ .$$

Then for each χ, $\hat{v}_\chi$ lies in $\hat{B}$. Moreover, the mapping

$$\begin{aligned} \hat{G} &\to \hat{B} \\ \chi &\mapsto \hat{v}_\chi \end{aligned}$$

is a bijection.

Note that the proposition subsumes the assertion that the Fourier transform of the convolution $f*g$ is the complex product of Fourier transforms $\hat{f}\hat{g}$.

PROOF. Clearly each ν_χ is linear on $L^1(G)$, and not identically zero, since each character χ of G takes values of norm 1. We check with a routine calculation that each such map is multiplicative:

$$\begin{aligned}
\nu_\chi(f*g) &= \int f*g(y)\overline{\chi(y)}\,dy \\
&= \int\int f(z^{-1}y)g(z)dz\,\overline{\chi(y)}\,dy \\
&= \int\int f(z^{-1}y)\overline{\chi(y)}\,dy\,g(z)\,dz \\
&= \int\int f(y)\overline{\chi(zy)}\,dy\,g(z)\,dz \\
&= \int f(y)\overline{\chi(y)}\,dy \int g(z)\overline{\chi(z)}\,dz \\
&= \hat{f}(\chi)\hat{g}(\chi) \;.
\end{aligned}$$

We show next that every nonzero character of B is of the form ν_χ for some group character χ. Let $\psi: B \to \mathbf{C}$ be a nontrivial algebra homomorphism. By Gelfand theory (Lemma 2-10) we know that ψ is a functional on $L^1(G)$ of norm bounded by 1. Hence by the duality of L^1 and L^∞ there exists some $\varphi \in L^\infty(G)$ having identical norm such that

$$\psi(f) = \int_G f(x)\varphi(x)dx$$

for all $f \in L^1(G)$. Recall that for any $y \in G$ and function f defined on G, $L_y f$ is defined by $L_y f(x) = f(y^{-1}x)$. Now compute:

$$\begin{aligned}
\int \psi(f)g(y)\varphi(y)\,dy &= \psi(f)\psi(g) \\
&= \psi(f*g) \\
&= \iint f(y^{-1}x)g(y)\,dy\,\varphi(x)dx \\
&= \iint L_y f(x)\varphi(x)\,dx\,g(y)dy \\
&= \int \psi(L_y f)g(y)\,dy \;.
\end{aligned}$$

Thus we have that

$$\psi(f)\varphi(y) = \psi(L_y f) \tag{3.4}$$

for almost all $y \in G$. One shows readily that the expression on the right is continuous in y—the elements of $\mathscr{C}_c(G)$ are dense in $L^1(G)$ and left and right uniformly continuous—whence we may assume that φ is likewise continuous; here

we need that ψ is not zero. Now applying the previous equation three times, we obtain

$$\psi(f)\varphi(xy) = \psi(L_{xy}f) = \psi(L_x L_y f) = \psi(L_y f)\varphi(x) = \psi(f)\varphi(x)\varphi(y) \quad .$$

Again since ψ is nonzero, φ is multiplicative on G. Thus in particular,

$$\varphi(y^{-1}) = \varphi(y)^{-1}$$

whence $|\varphi(y)|=1$ for all $y \in G$, because φ has L^{∞}-norm bounded by 1. This shows that φ is indeed a character of G and that $\psi = \hat{v}_{\bar{\varphi}}$.

Finally, given two group characters χ and χ', if $v_{\chi}(f) = v_{\chi'}(f)$ for all functions $f \in L^1(G)$, then by duality, χ and χ' must agree almost everywhere in G. But since both are continuous by definition, it follows that $\chi = \chi'$, as required. ☐

The Ring of Fourier Transforms and the Transform Topology

Consider now the space $\hat{A}$ [or, more explicitly, $\hat{A}(G)$, should we wish to emphasize the underlying locally compact abelian group G] defined by

$$\hat{A} = \{\hat{f} : f \in L^1(G)\} \quad .$$

Thus $\hat{A}$ consists of the Fourier transforms of functions $f \in L^1(G)$ and incidentally defines a weak topology on $\hat{G}$, the space of complex characters of G; this is the weakest topology such that each $\hat{f} \in \hat{A}$ is continuous. We shall call this the *transform topology* on $\hat{G}$. Since the Fourier transform of $f * g$ is the complex product of functions $\hat{f}\hat{g}$, it follows that $\hat{A}$ in fact constitutes a ring of continuous functions on $\hat{G}$ with respect to the transform topology. Now, according to the previous proposition, each element $\hat{f} \in \hat{A}$ may be regarded as the Gelfand transform of f insofar as we identify $\hat{G}$ with the space of characters on $L^1(G)$ via the mapping $\chi \mapsto \hat{v}_{\chi}$. More precisely, we have by construction that

$$\hat{f}(\hat{v}_{\chi}) = \hat{v}_{\chi}(f) = \hat{f}(\chi)$$

where, strictly speaking, on the left $\hat{f}$ denotes the Gelfand transform operating on the space of characters of $L^1(G)$ in the sense of Chapter 2, and on the right $\hat{f}$ denotes the Fourier transform operating on $\hat{G}$. These considerations lead at once to the following proposition.

3-12 PROPOSITION. *Let $\hat{G}$ have the transform topology induced by $\hat{A}$. Then the ring $\hat{A}$ is a separating, self-adjoint, dense subalgebra of $\mathscr{C}_0(\hat{G})$.*

PROOF. Let us first consider $\hat{B} = \mathrm{Hom}_{\mathbf{C}}(B,\mathbf{C})^*$. According to Lemma 2-10, if $L^1(G)$ is unital, then $\hat{B}$ is a (weakly) compact subset of the dual space B^*, and given $f \in L^1(G)$, its Gelfand transform $\hat{f}$ lies in $\mathscr{C}(\hat{B})$. Otherwise, $\hat{B}$ perhaps is not closed, because the weak limit of nontrivial algebra homomorphisms may in fact be trivial. Nonetheless, in either case $\hat{B}' = \hat{B} \cup \{0\}$ is closed. Thus for each $f \in L^1(G)$, we have that $\hat{f}$, when extended by zero to $\hat{B}'$, lies in $\mathscr{C}(\hat{B}')$, and therefore $\hat{f} \in \mathscr{C}_0(\hat{B})$.

Now identify $\mathscr{C}(\hat{G})$ with $\mathscr{C}(\hat{B})$ according to the topological isomorphism induced by $\chi \mapsto \hat{v}_\chi$. Then by Gelfand theory (Theorem 2-11 and Exercise 8 of Chapter 2) it follows that $\hat{A}$ is at least contained in $\mathscr{C}_0(\hat{G})$ and separates points. Thus it only remains to show that $\hat{A}$ is self-adjoint, since its density in $\mathscr{C}_0(\hat{G})$ is then a consequence of the Stone-Weierstrass theorem (see Proposition 2-13 and Exercise 9 below). Let $f \in L^1(G)$. Then for all characters χ on G, we have

$$\begin{aligned}\int \bar{f}(y^{-1})\overline{\chi(y)}\,dy &= \overline{\int f(y)\chi(y^{-1})\,dy}\\ &= \overline{\int f(y)\overline{\chi(y)}\,dy}\\ &= \bar{\hat{f}}(\chi)\end{aligned}$$

showing that $\hat{A}$ is indeed closed under complex conjugation, as required. ❑

This application of Gelfand theory becomes even more compelling in consideration of the following theorem:

3-13 THEOREM. *Let G and $\hat{G}$ be as above, and let K denote a compact subset of G, and V an open neighborhood of 1 in S^1. Then the following statements hold:*

(i) *Each of the sets $W(K,V)$ as defined in Section 3.1 is an open subset of $\hat{G}$ in the transform topology.*

(ii) *The system $\{W(K,V)\}$ in fact constitutes a neighborhood base for the trivial character with respect to the transform topology of $\hat{G}$.*

(iii) *The compact-open topology and the transform topology on $\hat{G}$ are identical.*

Note that (ii) immediately implies (iii), since by construction $\{W(K,V)\}$ is also a neighborhood base for the trivial character with respect to the compact-open topology. The proof will be straightforward, given the preliminary lemma that follows.

3-14 LEMMA. *Let $G \times \hat{G}$ have the product topology defined by the topology given on G and the corresponding transform topology on $\hat{G}$. Then*

(i) *For every $f \in L^1(G)$, the map*

$$G \times \hat{G} \to \mathbf{C}$$
$$(y, \chi) \mapsto (L_y f)^\wedge(\chi)$$

is continuous. [Here $(L_y f)^\wedge$ denotes the Fourier transform of the left translation of f by y.]

(ii) *The map*

$$G \times \hat{G} \to \mathbf{C}$$
$$(y, \chi) \mapsto \chi(y)$$

is likewise continuous.

PROOF. (i) Let (y_0, χ_0) be any fixed point in the domain of the given map. Then, according to Exercise 8 below, for every $\varepsilon > 0$, there exists a neighborhood U of y_0 such that

$$\| L_{y_0} - L_y \| < \varepsilon$$

for all $y \in U$. Moreover, by construction of the transform topology there exists a neighborhood V of χ_0 such that

$$|(L_{y_0} f)^\wedge(\chi) - (L_{y_0} f)^\wedge(\chi_0)| < \varepsilon$$

for all $\chi \in V$. Now since for any L^1-function g and character χ, $|\hat{g}(\chi)| \leq \|g\|_1$, it follows in particular that

$$|(L_y f)^\wedge(\chi) - (L_{y_0} f)^\wedge(\chi)| \leq \|L_y f - L_{y_0} f\|_1 \ .$$

Therefore,

$$|(L_y f)^\wedge(\chi) - (L_{y_0} f)^\wedge(\chi_0)| \leq |(L_y f)^\wedge(\chi) - (L_{y_0} f)^\wedge(\chi)| + |(L_{y_0} f)^\wedge(\chi) - (L_{y_0} f)^\wedge(\chi_0)| \leq 2\varepsilon$$

whenever $(y, \chi) \in U \times V$, and this clearly establishes the asserted continuity.

(ii) Note that Eq. 3.4 is equivalent, in the special case $\varphi = \bar{\chi}$, to the equation

$$\hat{f}(\chi)\bar{\chi}(y) = (L_y f)^\wedge(\chi) \ .$$

Exercise 9 shows that for every χ there is an L^1-function whose Fourier transform does not vanish at χ and hence does not vanish in a neighborhood of χ under the transform topology. Thus this last equation implies that the function $(y,\chi)\mapsto\overline{\chi}(y)$ on the product space is, according to part (i), the quotient of two continuous functions. Therefore both this function and its conjugate are likewise continuous. This completes the proof. ❑

PROOF OF THEOREM 3-13. According to our preliminary remarks, we need only prove parts (i) and (ii). Moreover, it clearly suffices to deal with subsets $W(K,V)$ of the form $W(K,N(\varepsilon))$, where the neighborhoods of the identity $N(\varepsilon)\subseteq S^1$, $\varepsilon>0$, are defined as in Section 3.1.

(i) Let K be a compact subset of G, and let $\varepsilon>0$ be given; choose and fix $\chi_0\in W(K,N(\varepsilon))$. Then in consequence of the preceding lemma, for every $y_0\in K$ there exist open neighborhoods U of y_0 in G and V of χ_0 in $\hat{G}$ (with respect to the transform topology) such that $\chi(y)\in N(\varepsilon)$ for all $\chi\in V$ and $y\in U$. The compact subset K is covered by finitely many open sets $U_1,\ldots,U_r$ with corresponding character sets $V_1,\ldots,V_r$. Clearly the intersection of the V_j is an open neighborhood of χ_0 contained in $W(K,N(\varepsilon))$, and therefore $W(K,N(\varepsilon))$ is open in $\hat{G}$, as claimed.

(ii) Let V be an open neighborhood of the trivial character, here denoted 1. We must show that V contains a subset of the form $W(K,N(\varepsilon))$ for some compact subset K of G and some positive ε. But by definition of the transform topology (consider its subbase!) we know that for some $\varepsilon_1>0$ there must indeed exist a finite family of functions $f_1,\ldots,f_r\in L^1(G)$ such that

$$\bigcap_j \{\chi : |\hat{f}_j(\chi)-\hat{f}_j(1)|<\varepsilon_1\}\subseteq V\ .$$

Since $\mathscr{C}_c(G)$ is dense in $L^1(G)$, we may further assume, at the cost of decreasing ε_1, that each of the f_j has compact support K_j. Let K denote the (necessarily compact) union of the K_j and choose a positive ε subject to the inequality

$$\varepsilon<\frac{3\varepsilon_1}{\max_j\|f_j\|_1}\ .$$

An easy calculation now shows that if $\chi\in W(K,N(\varepsilon))$, then for all j,

$$|\hat{f}_j(\chi)-\hat{f}_j(1)|<\varepsilon_1$$

whence $\chi\in V$. Hence V contains a subset of the required form, and the proof is complete. ❑

The Fourier Transform of a Character Measure

We continue with G and $\hat{G}$ as above. Let $\hat{\mu}$ be a Radon measure on $\hat{G}$ such that $\hat{\mu}(\hat{G})$ is finite. (Recall that a measure that is finite on the totality of its ambient space is said to have *finite total mass*). For $y \in G$, define

$$T_{\hat{\mu}}(y) = \int \chi(y) d\hat{\mu}(\chi) \quad .$$

We call this the *Fourier transform of the measure* $\hat{\mu}$. From the assumption that $\hat{\mu}$ has finite total mass, one deduces at once that this transform is both continuous and bounded by $\hat{\mu}(\hat{G})$ on G. Moreover, an application of Fubini's theorem shows that for all $f \in L^1(G)$,

$$\int \overline{\hat{f}(\chi)} d\hat{\mu}(\chi) = \int \overline{f(y)} T_{\hat{\mu}}(y) dy \quad . \tag{3.5}$$

The conditions for Fubini's theorem certainly hold since, $\hat{f}$ is bounded on $\hat{G}$ and the product $f(y)\overline{\chi}(y)$ is measurable on $G \times \hat{G}$ by the previous lemma.

3-15 PROPOSITION. *If for* $T_{\hat{\mu}}(y) = 0$ *every* $y \in G$, *then* $\hat{\mu} = 0$. *Thus* $\hat{\mu}$ *is completely determined by its Fourier transform.*

PROOF. According to Eq. 3.5, the hypothesis implies that

$$\int \overline{\hat{f}(\chi)} d\hat{\mu}(\chi) = 0$$

for all $f \in L^1(G)$. But recall that the ring of Fourier transforms of L^1-functions is dense in $\mathscr{C}_0(\hat{G})$. Hence, in particular,

$$\int g(\chi) d\hat{\mu}(\chi) = 0$$

for all continuous functions g on $\hat{G}$ with compact support. The result then follows at once by the elementary correspondence between Radon measures and integrals. ❑

This brings us to a key result—in fact, an amazing connection between measures on the character space of G and functions of positive type.

3-16 THEOREM. (Bochner) *The functions of* $\mathscr{P}(G)$ *(that is, the continuous functions of positive type on G with infinity norm less than or equal to* 1*)*

are precisely the Fourier transforms of Radon measures on $\hat{G}$ of total mass less than or equal to 1.

PROOF. First note that by Exercise 10 below, the Radon measures of finite total mass on a locally compact Hausdorff space correspond bijectively with the Radon measures on its one-point compactification that take the value zero on $\{\infty\}$. Now let $\hat{M}$ denote the set of Radon measures on $\hat{G}$ of total mass less than or equal to 1. If $\hat{\mu} \in \hat{M}$ is a point measure of total mass 1 concentrated at χ, then of course

$$T_{\hat{\mu}}(y) = \int \chi(y)d\hat{\mu}(\chi) = \chi(y)$$

whence the Fourier transform of $\hat{\mu}$ is precisely the character χ itself, and thus manifestly a function of positive type. Next suppose that $\hat{\mu}_0$ is the weak limit of arbitrary measures $\hat{\mu} \in \hat{M}$, by which we mean that corresponding Radon integrals converge pointwise on $\mathscr{C}(G')$. Then certainly

$$\int 1\, d\hat{\mu}_0 \leq 1$$

and thus the space $\hat{M}$ is weakly closed and therefore compact by Alaoglu's theorem. If $f \in L^1(G)$, we know that $\hat{f} \in \mathscr{C}(G')$, whence by definition of the weak convergence of measures,

$$\int \bar{\hat{f}}(\chi)\, d\mu_0 = \lim_{\mu} \int \bar{\hat{f}}(\chi)\, d\mu \quad .$$

From this and Eq. 3.5 we find that

$$\int \bar{f}(y) T_{\hat{\mu}_0}(y)\, dy = \lim_{\mu} \int \bar{f}(y) T_{\hat{\mu}}(y)\, dy$$

which is to say that $T_{\hat{\mu}_0}$ is the weak limit of $T_{\hat{\mu}}$, again owing to the density of the Fourier transforms in $\mathscr{C}_0(\hat{G})$. This is the key, for it has the following consequences:

(i) Since the every element of $\hat{M}$ is the weak limit of a linear combination of point measures of total mass 1 with positive coefficients (see Exercise 11 below), the Fourier transform of each measure in $\hat{M}$ is the weak limit of a linear combination of characters with positive coefficients, and therefore lies in the weakly closed set $\mathscr{P}(G)$.

(ii) The Fourier transform is a weakly continuous map from $\hat{M}$ to $\mathscr{P}(G)$, and hence its image is a weakly compact and, in particular, weakly closed subset of $\mathscr{P}(G)$. Moreover, this image is evidently convex and contains the characters of G as well as the zero function. Hence by Exercise 6, it must be precisely $\mathscr{P}(G)$ itself.

This completes the proof. ❑

Recall that $V=V(G)$ denotes the complex linear span of the continuous functions of positive type on G and that such functions are bounded, since a continuous function of positive type obtains its maximum at the identity of G. According to Bochner's theorem and the proposition that precedes it, each function $f\in V$ determines a measure $\hat{\mu}_f$ of finite total mass on $\hat{G}$ such that f is the Fourier transform of $\hat{\mu}_f$. This is to say,

$$f(y)=\int \chi(y)d\hat{\mu}_f(\chi)$$

for all $y\in G$.

The association of f with the measure $\hat{\mu}_f$ enjoys the following reciprocity law:

3-17 LEMMA. *Let f and g lie in $V^1=V\cap L^1(G)$. Then we have the equality of measures*

$$\hat{g}(\chi)d\hat{\mu}_f(\chi)=\hat{f}(\chi)d\hat{\mu}_g(\chi) \quad .$$

PROOF. Since these measures are completely determined by their Fourier transforms, it suffices to establish the equality for the corresponding transforms. This leads to a brief, but beautiful, exercise in integration, which depends primarily on Fubini's Theorem and the construction of $\hat{\mu}_f$ and $\hat{\mu}_g$:

$$\begin{aligned} T_{\hat{g}(\chi)d\hat{\mu}_f(\chi)}(y) &= \int \chi(y)\ \hat{g}(\chi)\,d\hat{\mu}_f(\chi) \\ &= \int \chi(y)\int g(z)\overline{\chi(z)}dz\, d\hat{\mu}_f(\chi) \\ &= \int\int \chi(z^{-1}y)d\hat{\mu}_f(\chi)\ g(z)\,dz \\ &= \int f(z^{-1}y)\ g(z)\,dz \\ &= f*g(y) \quad . \end{aligned}$$

Thus the Fourier transform of the left-hand side of the asserted equality of measures is precisely the convolution $f*g$, and by symmetry the Fourier transform of the right-hand side is precisely $g*f$. But naturally, these convolutions are equal, whence the equality of measures, as claimed. ❑

Let $\mathscr{F}$ denote the set of continuous, bounded, complex-valued functions φ on $\hat{G}$ that satisfy the following condition: there exists some complex measure $\hat{\nu}_\varphi$ on $\hat{G}$ of finite total mass such that

$$\varphi(\chi)\,d\hat{\mu}_f(\chi) = \hat{f}(\chi)\,d\hat{\nu}_\varphi(\chi)$$

for all $f \in V^1$. According to the previous lemma, the Fourier transforms of elements of V^1 certainly lie in $\mathscr{F}$: if $\varphi = \hat{g}$ for some $g \in V^1$, then $\hat{\nu}_\varphi$ is simply $\hat{\mu}_g$.

As our final preliminary to the proof of the Fourier inversion formula, we establish some key properties of the set $\mathscr{F}$.

3-18 LEMMA. *The set $\mathscr{F}$ defined above has the following properties:*

(i) *If $\varphi \in \mathscr{F}$, the associated measure $\hat{\nu}_\varphi$ is unique.*

(ii) *If $\varphi \in \mathscr{F}$ arises as the Fourier transform of an element $f \in L^1(G)$, then $\hat{\nu}_\varphi = \hat{\mu}_f$.*

(iii) *If $\varphi \in \mathscr{F}$ is positive, then the measure $\hat{\nu}_\varphi$ is likewise positive.*

(iv) *The set $\mathscr{F}$ constitutes a module over the ring of continuous, bounded, complex-valued functions on $\hat{G}$; moreover, with respect to this module structure, the mapping $\varphi \mapsto \hat{\nu}_\varphi$ constitutes a homomorphism of modules into the space of complex measures on $\hat{G}$ of finite total mass, viewed as a module over the same ring of continuous bounded functions. In particular, we have that*

$$\hat{\nu}_{\varphi+\gamma} = \hat{\nu}_\varphi + \hat{\nu}_\gamma \quad \textit{and} \quad \hat{\nu}_{a\varphi} = a\,\hat{\nu}_\varphi$$

for all $\varphi, \gamma \in \mathscr{F}$ and continuous bounded functions a on $\hat{G}$.

(v) *If $\varphi \in \mathscr{F}$, then every translation γ of φ also lies in $\mathscr{F}$, and to obtain $\hat{\nu}_\gamma$ from $\hat{\nu}_\varphi$ one applies the same translation. In particular, if $f \in L^1(G)$ and g is obtained from f by multiplication by a character χ_0, then the associated functions $\hat{g}$ and $\hat{\mu}_g$ are obtained from $\hat{f}$ and $\hat{\mu}_f$ respectively via translation by χ_0.*

PROOF. (i) Let $\varphi \in \mathscr{F}$. According to Exercise 12 below, there exists a net of functions f in $V^1(G)$ such that $\hat{f}$ converges uniformly to the constant function 1 on compact subsets of $\hat{G}$. By construction it then follows that

$$\lim_f \varphi(\chi) d\hat{\mu}_f(\chi) = d\hat{\nu}_\varphi(\chi)$$

and therefore $\hat{\nu}_\varphi$ is uniquely determined by φ.

(ii) This follows at once from part (i) and the preceding lemma.

(iii) This essentially follows from the argument made in part (i) with one additional observation: according to Bochner's theorem, the measures $\hat{\mu}_f$ that arise in connection with the net f are each positive. Hence if φ is positive, $\hat{\nu}_\varphi$ is the limit of positive measures $\varphi(\chi)d\hat{\mu}_f(\chi)$ and hence itself positive.

(iv) The additivity of the map $\varphi \mapsto \hat{\nu}_\varphi$ is obvious from the uniqueness statement. Along the same lines, if a is continuous and bounded on the space of characters of G, then the equality

$$a(\chi)\varphi(\chi)\, d\hat{\mu}_f(\chi) = \hat{f}(\chi)a(\chi)\, d\hat{\nu}_\varphi(\chi)$$

shows at once that $\hat{\nu}_{a\varphi} = a\hat{\nu}_\varphi$. These facts taken together show that $\mathscr{F}$ is a module over the given ring and that the map $\varphi \mapsto \hat{\nu}_\varphi$ is a module homomorphism.

(v) The issue here is not so much mathematics as typography. Hence we introduce the following provisional notation: if μ is a measure on a group and z is any group element, we shall write μ^z for the left translation of μ by z. That is, if E is any measurable subset of the ambient group, then $\mu^z(E) = \mu(z^{-1}E)$.

Fix a character χ_0 and define the translation γ of φ by $\gamma(\chi) = \varphi(\chi_0^{-1}\chi)$. With the convention above in force, we make the following calculation, leaving the details to the reader. For all $h \in \mathscr{C}_c(\hat{G})$ and $f \in L^1(G)$,

$$\begin{aligned}
\int h(\chi)\gamma(\chi)d\hat{\mu}_f(\chi) &= \int h(\chi)\varphi(\chi_0^{-1}\chi)d\hat{\mu}_f(\chi) \\
&= \int h(\chi_0\chi)\varphi(\chi)d\hat{\mu}_f^{\chi_0^{-1}}(\chi) \\
&= \int h(\chi_0\chi)\varphi(\chi)d\hat{\mu}_{\chi_0^{-1}f}(\chi)
\end{aligned}$$

$$= \int h(\chi_0\chi)(\chi_0^{-1}f)^\wedge(\chi)d\hat{v}_\varphi(\chi)$$
$$= \int h(\chi_0\chi)\hat{f}(\chi_0\chi)d\hat{v}_\varphi(\chi)$$
$$= \int h(\chi)\hat{f}(\chi)d\hat{v}_\varphi^{\chi_0}(\chi) \ .$$

Hence

$$\gamma(\chi)d\hat{\mu}_f(\chi) = \hat{f}(\chi)d\hat{v}_\varphi^{\chi_0}(\chi)$$

showing that $\hat{v}_\gamma$ is the required translation of $\hat{v}_\varphi$. ❑

Proof of the Fourier Inversion Formula

The proof of the inversion formula proper now requires three steps. We defer the identification of $V^1(G)$ with $V^1(\hat{G})$ via the Fourier transform until the following section.

First we claim that a function γ that lies in $\mathscr{C}_c(\hat{G})$ also lies in $\mathscr{F}$. Let K be a compact subset of the space of characters that contains the support of γ. Then we may assert, as in part (i) of the preceding lemma, that there exists a function $f \in V^1(G)$ whose Fourier transform is bounded away from zero on K. Hence the quotient $a = \gamma / \hat{f}$ is bounded and continuous on K and may be extended to a bounded continuous function on the full space of characters by simply defining it to be zero on the complement of K. Since the Fourier transform of f lies in $\mathscr{F}$, it follows by part (iv) of the previous result that γ likewise lies in $\mathscr{F}$, as promised.

The second step amounts to the choice of a Haar measure for the character space. First consider the mapping

$$\begin{aligned} \mathscr{C}_c(\hat{G}) &\overset{\eta}{\to} \mathbf{C} \\ \gamma &\mapsto \int 1 \, d\hat{v}_\gamma(\chi) \ . \end{aligned}$$

If $f \in V^1(G)$ is not identically zero, then neither is the associated measure $\hat{\mu}_f$, which is to say that there exists a continuous, bounded function a on the character space such that the measure $a(\chi)d\hat{\mu}_f(\chi)$ is also nonzero. But then taking γ to be the product $a\hat{f}$, we have that $d\hat{v}_\gamma = a(\chi)d\hat{\mu}_f(\chi)$, whence the mapping η is not the zero map. The upshot is this: since η is not the zero map, it follows from parts (iii), (iv), and (v) of the lemma that η is in fact a Haar measure $d\chi$

on $\hat{G}$. In particular, the translation-invariance follows from part (v) by the following calculation:

$$\int 1\, d\hat{\nu}_{L_{\chi_0}\gamma}(\chi) = \int 1\, d\hat{\nu}_{\gamma}^{\chi_0}(\chi) = \int L_{\chi_0^{-1}} 1\, d\hat{\nu}_{\gamma}(\chi) = \int 1\, d\hat{\nu}_{\gamma}(\chi) \ .$$

Thus with respect to this measure we may write

$$\int \gamma(\chi) d\chi = \int d\hat{\nu}_{\gamma}(\chi)$$

for all γ in $\mathscr{C}_c(\hat{G})$.

To begin the final step, note that for all $\varphi \in \mathscr{F}$ and $a \in \mathscr{C}_c(\hat{G})$ the product $a\varphi$ of course also has compact support. Thus according to the preceding equation and part (iv) of the lemma,

$$\int a(\chi)\varphi(\chi) d\chi = \int a(\chi) d\hat{\nu}_{\varphi}(\chi) \ .$$

This is to say that

$$\varphi(\chi) d\chi = d\hat{\nu}_{\varphi}(\chi) \ .$$

But then, in particular, for $f \in V^1(G)$,

$$\hat{f}(\chi) d\chi = d\hat{\mu}_f(\chi)$$

and hence by construction,

$$f(y) = \int \chi(y) d\hat{\mu}_f(\chi) = \int \hat{f}(y)\chi(y) d\chi \ .$$

This establishes the formula. ❑

We conclude this section with a fine corollary that prepares the way for the identification of $V^1(G)$ with $V^1(\hat{G})$.

3-19 COROLLARY. *Let f be a complex-valued function on G that is integrable with respect to the Haar measure dx on G. Then the following statements hold:*

(i) *If f is moreover continuous and of positive type, then the Fourier transform of f is a positive function on the space of characters of G.*

(ii) *For f as in the previous part we also have that*

$$\int f(x)dx \geq 0 \quad .$$

(iii) *If f is positive on G, then its Fourier transform is a function of positive type.*

Thus the Fourier transform defines an injective mapping from $V^1(G)$ *to* $V^1(\hat{G})$.

PROOF. (i) By the inversion formula, f is precisely the Fourier transform of the character measure $\hat{f}(\chi)d\chi$. According to Bochner's theorem, this must be a Radon measure of finite total mass, and, in particular, positive. Hence the Fourier transform of f, being continuous, must also be positive.

(ii) This is a particular instance of part (i):

$$\int f(x)dx = \hat{f}(1) \geq 0 \quad .$$

Here 1 denotes the identity character.

(iii) We leave this to the reader as an exercise in direct calculation.

The final statement now follows directly from part (iii) by linearity: Each element in $V^1(G)$ can be written as a complex linear combination of positive integrable functions. Hence the Fourier transform indeed defines a mapping into the stated codomain; it is, of course, injective by the inversion formula. □

Henceforth we assume that the Haar measures on G and its dual are normalized so that the Fourier inversion formula holds.

3.4 Pontryagin Duality

Again let G denote a locally compact abelian group, with character group $\hat{G}$, which, as we have seen, is also locally compact and abelian. We can thus iterate the operation of taking the dual and define a natural map

$$\alpha : G \to \hat{\hat{G}}, \quad \alpha(y)(\chi) = \chi(y) \quad .$$

That is, $\alpha(y)$ is just evaluation at y on the dual space. This is clearly a (continuous) character of $\hat{G}$. The main point of this section is to establish the following result:

3-20 THEOREM. (Pontryagin Duality) *The map $\alpha: G \to \hat{\hat{G}}$ is an isomorphism of topological groups. Hence G and $\hat{G}$ are mutually dual.*

We begin with a lemma that shows that the map α is at least injective. This will subsequently allow us to identify its image with a subset of G.

3-21 LEMMA. *The mapping α defined above is injective; that is, $\hat{G}$ separates points in G.*

PROOF. Suppose that z is not the identity of G. Clearly it suffices to demonstrate the existence of a character χ such that $\chi(z) \neq 1$. Suppose that no such χ exists. Then by definition of the Fourier transform and Haar measure, it is immediate that

$$\hat{f} = (L_z f)^\wedge$$

for all f in $L^1(G)$. Hence by the Fourier inversion formula we get $f = L_z f$ for all f in $V^1(G)$. Now, since G is Hausdorff, there exists an open neighborhood U of the identity such that $U \cap (z^{-1}U) = \varnothing$. By Exercise 5, there exists a nonzero continuous function f of positive type with support in U. But for such f, it is impossible that $f = L_z f$. The contradiction completes the proof. ❑

Now let $\hat{K}$ be a compact neighborhood of the identity character in $\hat{G}$. Given an open neighborhood V of the identity in S^1, we may apply the construction of Section 3.1 to define the following subset of the double dual of G:

$$W(\hat{K}, V) = \{\psi \in \hat{\hat{G}} : \psi(\chi) \in V \text{ for all } \chi \in \hat{K}\} \quad .$$

Such subsets and their translates constitute a base for the topology of $\hat{\hat{G}}$. Of course, some of the elements in the double dual arise unambiguously from elements of G via the mapping α. Hence it makes sense to define

$$W_G(\hat{K}, V) = W(\hat{K}, V) \cap \alpha(G)$$

and to regard this as a subset of G. We shall use these subsets to characterize the topology of G in a way that immediately implies that α is moreover a homeomorphism onto its image.

3-22 PROPOSITION. *The subsets $W_G(\hat{K},V)$ and their translates constitute a base for the topology of G.*

PROOF. Let U be an open neighborhood of the identity $e\in G$. Then again by Exercise 5, there exists a continuous function g on G of positive type with support in U such that $g(e)=1$. It follows from Corollary 3-19, part (i), that the Fourier transform of g is positive. Moreover, from the inversion formula we have

$$\int \hat{g}(\chi)d\chi = 1 \ .$$

Thus we may identify $\hat{g}(\chi)d\chi$ with a finite Radon measure on $\hat{G}$, which in particular is inner regular. Accordingly, given any positive ε there exists a compact subset $\hat{K}$ of characters such that

$$\int_{\hat{K}} \hat{g}(\chi)d\chi > 1-\varepsilon$$

and hence the corresponding integral over the complement of $\hat{K}$ is less than ε. Now consider the identity

$$g(y) = \int_{\hat{K}} \hat{g}(\chi)\chi(y)d\chi + \int_{\hat{K}^c} \hat{g}(\chi)\chi(y)d\chi$$

given by the Fourier inversion formula. As V shrinks to a sufficiently small neighborhood of 1 in S^1, the first integral above eventually lies within ε of unity for all $y\in W_G(\hat{K},V)$, while the second is unconditionally bounded in absolute value by ε. Hence g must be bounded from below by $1-2\varepsilon$ on $W_G(\hat{K},V)$. But by construction, U contains the support of g, and therefore U contains $W_G(\hat{K},V)$, thus completing the proof. ❑

3-23 COROLLARY. *The mapping α defined above is bicontinuous; thus α is a homeomorphism onto its image.*

PROOF. By construction we have the identity

$$\alpha(W_G(\hat{K},V)) = W(\hat{K},V)\cap\alpha(G)$$

which in light of the lemma and the proposition shows that α is bicontinuous at the identity element of G. Since α is clearly a group isomorphism onto its image, the result holds everywhere in G by translation. ❑

Recalling one of the fundamental facts of topological groups, this first corollary nets us a second:

3-24 COROLLARY. *The image of α is closed in $\hat{\hat{G}}$.*

PROOF. By general topology, a locally compact and dense subset of a Hausdorff space must be open. Now $\alpha(G)$ is locally compact, being the homeomorphic image of the locally compact group G, and, of course, is dense in its closure in the double dual. Accordingly, $\alpha(G)$ is an open subgroup of its closure. But since every open subgroup of a topological group is also closed, $\alpha(G)$ is in fact identical to its closure, as required. □

Given these two corollaries, the proof of Pontryagin's theorem reduces to showing that $\alpha(G)$ is dense in the double dual of G. This requires a final bit of delicate analysis.

The Plancherel Theorem

Let $f \in L^1(G)$ and as usual, define $\tilde{f}(x) = \overline{f(x^{-1})}$ for $x \in G$. An easy calculation shows that

$$\hat{\tilde{f}}(\chi) = \overline{\hat{f}(\chi)} \ .$$

Set $g = f * \tilde{f}$; then certainly g is integrable and moreover, according to Exercise 5 below, of positive type. If f lies also in $L^2(G)$, the Fourier inversion formula yields the following key observation:

$$\begin{aligned} \int |f(x)|^2 \, dx &= g(1) \\ &= \int \hat{g}(\chi) \, d\chi \\ &= \int |\hat{f}(\chi)|^2 \, d\chi \ . \end{aligned}$$

This shows that the Fourier transform induces a map

$$\begin{aligned} L^1(G) \cap L^2(G) &\to L^2(\hat{G}) \\ f &\mapsto \hat{f} \end{aligned}$$

which is an isometry onto its image.

Recall that $\hat{A} = \hat{A}(G)$ denotes the ring of Fourier transforms of functions in $L^1(G)$. Let $\hat{A}_1$ denote the subset of $\hat{A}$ arising from the isometry above. Note that $\hat{A}_1$ is stable under multiplication by elements of $\alpha(G)$:

$$\begin{aligned}[\alpha(y_0)\cdot\hat{f}](\chi) &= \chi(y_0)\int f(y)\bar{\chi}(y)\,dy \\ &= \int f(y)\bar{\chi}(y_0^{-1}y)\,dy \\ &= \int f(y_0 y)\bar{\chi}(y)\,dy \\ &= (L_{y_0}f)\hat{}(\chi) \ .\end{aligned}$$

The following result is the key to our current discussion.

3-25 LEMMA. *$\hat{A}_1$ is a dense subspace of the Hilbert space $L^2(\hat{G})$.*

Granting this, since also $L^1(G)\cap L^2(G)$ is dense in $L^2(G)$—the intersection contains $\mathscr{C}_c(G)$—the isometry defined by the restricted Fourier transform may be extended by continuity to an isometric isomorphism

$$\begin{aligned} L^2(G) &\to L^2(\hat{G}) \\ f &\mapsto \hat{f} \ . \end{aligned}$$

Note that we continue to use the circumflex notation for this extended version of the Fourier transform, called the *Plancherel transform*. To summarize, relative to the preceding lemma, we have established the following:

3-26 THEOREM. (Plancherel) *Let G be a locally compact abelian group. Then the extended Fourier transform defines an isometry of Hilbert spaces from $L^2(G)$ onto $L^2(\hat{G})$.* ❑

PROOF OF LEMMA. In view of the self-duality of Hilbert spaces and the Hahn-Banach theorem, it suffices to show that zero is the only element of $L^2(\hat{G})$ orthogonal to every element of $\hat{A}_1$.

Assume that $g\in L^2(\hat{G})$ is orthogonal to every element in $\hat{A}_1$. Since $\hat{A}_1$ is stable under multiplication by elements of $\alpha(G)$ for all $f\in\hat{A}_1$ and $y\in G$, we have that

$$\int g(\chi)\bar{f}(\chi)\chi(y)\,d\chi = 0 \ .$$

This says that the Fourier transform of the measure $g(\chi)\bar{f}(\chi)d\chi$ is zero, and hence by a slight extension of Proposition 3-15 so is the product $g\bar{f}$ almost everywhere. But note that for a character χ we have $(\chi\cdot f)\hat{} = L_\chi \hat{f}$. Thus given *any* nonzero continuous element of $\hat{A}_1$, we can produce an element of $\hat{A}_1$ that does not vanish in some neighborhood of χ. Hence if the product $g\bar{f}$ is zero almost everywhere, it must be that g is zero in $L^2(\hat{G})$, as required. ❑

3-27 COROLLARY. (Parseval's Identity) *For all $f,g\in L^2(G)$, we have*

$$\int f(x)\bar{g}(x)\,dx = \int \hat{f}(\chi)\bar{\hat{g}}(\chi)\,d\chi \quad .$$

PROOF. By elementary linear algebra, a linear isometry is necessarily unitary. ❑

3-28 COROLLARY. *Let f and g lie in $L^2(G)$, and let h lie in $L^1(G)$. Then if $h=f\cdot g$, we have $\hat{h}=\hat{f}*\hat{g}$.*

PROOF. Suppose that h factors as given. Let χ_0 be a character. We compute as follows, appealing to Parseval's identity to justify the transition from the second to the third line:

$$\begin{aligned}
\hat{h}(\chi_0) &= \int f(y)g(y)\bar{\chi}_0(y)\,dy \\
&= \int f(y)\overline{\bar{g}(y)\chi_0(y)}\,dy \\
&= \int \hat{f}(\chi)\hat{g}(\chi^{-1}\chi_0)\,d\chi \\
&= \hat{f}*\hat{g}(\chi_0) \quad .
\end{aligned}$$

This completes the proof. ❑

3-29 COROLLARY. *The ring $\hat{A}$ of Fourier transforms of L^1-functions on G consists precisely of convolutions of functions in $L^2(\hat{G})$.*

PROOF. If $h\in L^1(G)$, then h factors as $f\cdot g$ for functions $f,g\in L^2(G)$. For instance, $h=r\cdot|r|$ where $r\in L^2(G)$ is defined by

$$r(x)=\begin{cases} h(x)/|h(x)|^{1/2} & \text{if } h(x)\neq 0 \\ 0 & \text{otherwise.}\end{cases}$$

Hence $\hat{h} = \hat{f} * \hat{g}$, and therefore every element of $\hat{A}$ is of the required form. Conversely, by Plancherel's theorem every convolution of functions in $L^2(\hat{G})$ takes the form $\hat{f} * \hat{g}$ for some f and g as above, and hence is the transform of the L^1-function $f \cdot g$. Accordingly, such products lie in $\hat{A}$, as required. ❑

This brings us to the final technical prerequisite for the proof of Pontryagin's theorem.

3-30 PROPOSITION. *Let U be a nonempty open subset of $\hat{G}$. Then there exists a nonzero function $\hat{f} \in \hat{A}$ with support contained in U.*

PROOF. Recall from Proposition 1-7, part (iii), that the volume of any nonempty open set relative to a Haar measure is positive. Thus, by inner regularity, there exists a compact subset K of U with positive measure. At every point of $x \in K$ we can find an open neighborhood V_x of the identity and an open neighborhood U_x of x such that $U_x V_x$ is contained in U. Then since K is compact and $\hat{G}$ is locally compact, there exists a compact neighborhood V of the identity such that KV is contained in U. Define $\hat{f}$ as the convolution of the characteristic functions on K and V, respectively. It follows at once from the previous result that $\hat{f} \in \hat{A}$ and that $\hat{f}$ has support contained in KV, and therefore contained in U. Moreover, one calculates at once that the integral of $\hat{f}$ over $\hat{G}$ is simply the product of the measures of K and V, and hence positive. Thus $\hat{f}$ is nonzero on a set of positive measure. ❑

Proof of Pontryagin's Theorem

As we observed above, it remains only to show that $\alpha(G)$ is dense in $\hat{\hat{G}}$. If not, then according to our last proposition, there exists a function in $\varphi \in L^1(\hat{G})$ such that $\hat{\varphi}$ is nonzero but nonetheless $\hat{\varphi}$ vanishes on $\alpha(G)$. Let $\hat{\chi}_0$ lie in the double dual. Then by definition,

$$\hat{\varphi}(\hat{\chi}_0) = \int \varphi(\chi)\hat{\chi}_0(\chi^{-1})d\chi \ .$$

But the assumption that $\hat{\varphi}$ vanishes on $\alpha(G)$ means precisely that

$$\int \varphi(\chi)\chi(y^{-1})d\chi = 0$$

for all $y \in G$. Hence, as in the proof of Plancherel's theorem, $\varphi = 0$ almost everywhere, and therefore $\hat{\varphi} = 0$. This contradiction completes the proof. ❑

The only remaining issue in this chapter is to establish the last statement of the Fourier inversion formula, namely that the Fourier transform identifies $V^1(G)$ with $V^1(\hat{G})$. We have already shown that the map $f \mapsto \hat{f}$ is injective.

Let F lie in $V^1(\hat{G})$, and define a function f on G by the formula

$$f(y) = \int F(\chi)\chi(y)\,d\chi \quad .$$

Identifying G with $\hat{\hat{G}}$, this amounts to

$$f(y) = \hat{F}(y^{-1})$$

which places $f \in V^1(G)$ by Corollary 3-19. [One verifies at once from the definition that if $y \mapsto \varphi(y)$ is of positive type, then so is $y \mapsto \varphi(y^{-1})$.] By the Fourier inversion formula,

$$\begin{aligned} F(\chi) &= \int \hat{F}(y)\chi(y)\,dy \\ &= \int f(y^{-1})\chi(y)\,dy \\ &= \int f(y)\overline{\chi(y)}\,dy \end{aligned}$$

and this shows that F is the Fourier transform of f. Hence $f \mapsto \hat{f}$ is also surjective, as required. ❑

Exercises

1. Let G be a locally compact topological group. We consider functions from G into either the real or complex numbers.

(a) Let f_1 and f_2 be Haar-measurable functions on G. Show that the product $f_1 f_2$ is likewise Haar-measurable on G.

(b) Let f be a Haar-measurable function on G. Define F on $G \times G$ by

$$F(g,h) = f(g)f(h) \quad .$$

Show that F is Haar-measurable on $G \times G$.

(c) Let φ be a Haar-measurable function on G. Define ψ on $G\times G$ by

$$\psi(g,h) = \varphi(g^{-1}h) \ .$$

Show that ψ is Haar-measurable on $G\times G$.

2. Let G be a topological group and let X be a metric space, with $x_0 \in X$. Suppose that $f: G \to X$ is a continuous function subject to the condition that there exists a compact subset K of G such that if $s \notin K$, then $f(s) = x_0$. (Thus we generalize the idea of compact support to cases for which the codomain has no algebraic structure.) Use Proposition 1-1 to show that f is uniformly continuous in the following sense: for every $\varepsilon > 0$, there exists a neighborhood V of the identity in G such that $|f(s) - f(t)| < \varepsilon$ whenever $s^{-1}t \in V$.

3. Let $f \in \mathscr{C}_c(G)$ and let $g \in \mathscr{C}_0(G)$. Show that $f*g$ likewise lies in $\mathscr{C}_0(G)$. [*Hint*: For continuity, use an easy extension of Exercise 2 to show that if $t_\alpha \to t$ in G, then for any positive ε, eventually

$$\left|\int (g(s^{-1}t) - g(s^{-1}t_\alpha)) f(s)\, ds\right| < \|f\|_\infty \, \mu(\operatorname{supp} f)\varepsilon \ .$$

To see that $f*g$ moreover vanishes at infinity, note that for every positive ε there exists a compact subset K_0 of G such that $|g|$ is bounded by ε on K_0^{c}, the complement of K_0. But also, the support of f is confined to a compact subset K_1 of G. Now if t lies outside of the compact product $K = K_1K_0$, then whenever ts lies in K_1, s^{-1} must lie outside of K_0. Thus

$$\left|\int g(s^{-1}) f(ts)\, ds\right| < \|f\|_\infty \, \mu(K_1)\varepsilon$$

whence $f*g(t)$ tends to 0 as t tends to infinity.]

4. Let ρ be a unitary representation of a locally compact group G on a Hilbert space V. Let $x \in V$ be arbitrary. Show that the mapping

$$s \mapsto \langle x \,|\, \rho(s)[x] \rangle$$

is of positive type. This essentially establishes the converse of Proposition 3-4. [*Hint*: In the manner of the introductory discussion of Section 3.2, consider the discrete analogue of this statement.]

5. For f a complex-valued function defined on a locally compact abelian group G, define $\tilde{f}$, also on G, by

$$\tilde{f}(s) = \overline{f(s^{-1})} \quad .$$

Use the preceding exercise to show that if $f \in \mathscr{C}_c(G)$, then the convolution product $f * \tilde{f}$ is continuous of positive type on G. Next use Urysohn's lemma to show that for any open neighborhood V of the identity, there is a continuous function g of positive type with support contained in V such that $g(e)=1$.

6. Let G be a locally compact abelian group. Show that every closed, convex subset of $L^\infty(G)$ that contains the characters of G and the zero function also contains $\mathscr{P}(G)$. [*Hint*: Use Lemma 3-6 and Theorem 3-8.]

7. Show that for a locally compact *abelian* group G with Haar measure μ,

$$\mu(E) = \mu(E^{-1})$$

for all Borel subsets E. [*Hint*: Show that $\nu(E)=\mu(E^{-1})$ is likewise a Haar measure on G, hence a multiple λ of μ. But what if E is a symmetric subset of G of finite measure? Must such subsets exist?]

8. Let G be a locally compact abelian group. Use that $\mathscr{C}_c(G)$ is dense in $L^p(G)$ for $1 \le p \le \infty$ to show that for all $y \in G$ the mapping

$$\begin{aligned} L^1(G) &\to L^1(G) \\ f &\mapsto L_y f \end{aligned}$$

is uniformly continuous. [The same is true for $L^p(G)$, $1 \le p < \infty$.]

9. Let G be a locally compact abelian group. Show that for every character χ of G there exists a function $f \in L^1(G)$ such that $\hat{f}(\chi) \neq 0$. [*Hint*: The real part of χ is positive in some neighborhood of 1. Use the local compactness of G and Urysohn's lemma to construct an appropriate f.]

10. Let X be a locally compact Hausdorff space. Show that each Radon measure μ on X of finite total mass extends uniquely to a Radon measure μ' on X', the one-point compactification of X, such that $\mu'(\{\infty\})=0$. [*Hint*: To see that μ' is outer regular, observe that for E measurable,

$$\mu(E) \leq \inf \mu(U \cup U_\infty) \leq \inf (\mu(U) + \mu(U_\infty))$$

where the infimum is taken over all pairs of open sets U and U_∞ such that U contains E and U_∞ contains ∞. But since μ is inner regular on G, there exist neighborhoods of ∞ of arbitrarily small measure. Now derive the inner regularity of μ' from its outer regularity and the fact that a subset of X' is compact if and only if its complement is open; in essence the supremum calculation over compact subsets of E is equivalent to the infimum calculation over open supersets of E.]

11. Let G be a locally compact topological group (not necessarily abelian) and let μ be a positive Radon measure on G of finite total mass. Recall that we may identify μ with a linear functional on $\mathscr{C}_c(G)$, and that under this identification a point measure corresponds to a positive multiple of an evaluation map. As usual, G' denotes the one-point compactification of G, and μ is extended to G' by setting $\mu(\infty)=0$.

(a) Show that for every open neighborhood U of the identity in G and open neighborhood V of ∞ in G' there exists a finite partition of G consisting of measurable sets $W_1, \ldots, W_n, W_\infty$ such that each W_j admits a translate contained in U and W_∞ lies in V. [*Hint*: A finite number of translates of U cover the complement of V, and these together with $V - \{\infty\}$ cover G. Extract the required partition from this open cover.]

(b) Let U, V, and $W_1, \ldots, W_n$ be as above and select points $w_j \in W_j$ for $j=1,\ldots,n$. Define a corresponding linear functional $\mu_{U,V}$ on $\mathscr{C}_c(G)$ by

$$\mu_{U,V}(f) = \sum \mu(W_j) f(w_j) \quad .$$

Show that for each f in $\mathscr{C}_c(G)$, as U approaches the identity and V approaches ∞, $\mu_{U,V}(f)$ approaches $\mu(f)$. [*Hint*: Assuming that the support of f is contained in the complement of V, we have evidently that

$$\left|\int f\,d\mu - \mu_{U,V}(f)\right| \leq \sum \int_{W_j} |f(w) - f(w_j)|\,d\mu(w) \ .$$

Now use the finiteness of the mass of μ and the uniform continuity of f (cf. Section 1.1) to deduce the conclusion.]

(c) Conclude from parts (a) and (b) that every measure μ on G of the given type is the weak limit of a linear combination of point measures of total mass 1 with positive coefficients.

12. Let G be a locally compact abelian group. Show that there exists a net of functions f in $V^1(G)$ whose Fourier transforms converge uniformly to the constant function 1 on compact subsets of the space of characters on G. [*Hint*: Consider a compact neighborhood K of the identity and a positive function g_K having support on K whose integral is 1. What can one say about the convolution $f_K = g_K * \tilde{g}_K$, especially in light of Exercise 5?]

13. (Duality for Finite Abelian Groups) Let G be a finite abelian group, and set

$$\hat{G} = \mathrm{Hom}(G, S^1) \ .$$

Note that we may assume the discrete topology for G, whence continuity plays no role.

(a) Let $\mathbf{C}G$ denote the space of complex-valued functions on G; in other words, the complex group algebra of G. For every $f \in \mathbf{C}G$, define its *Fourier transform* by

$$\begin{aligned} \hat{f} : \hat{G} &\to \mathbf{C} \\ \chi &\mapsto \sum_{g \in G} f(g)\overline{\chi}(g) \, . \end{aligned}$$

Prove directly that

$$f(g) = \frac{1}{\mathrm{Card}(G)} \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(g) \ .$$

This is, of course, the finite version of the Fourier inversion formula.

(b) Show explicitly in the case $G = \mathbf{Z}/n\mathbf{Z}$ that also $\hat{G} = \mathbf{Z}/n\mathbf{Z}$. [*Hint*: If σ generates G, show that $\hat{G}$ is generated by the map $\chi: \sigma^k \mapsto e^{2\pi i k/n}$.]

(c) Let H be a subgroup of G, let $\mu \in \hat{H}$, and let $y \in G - H$. Set H' equal to the subgroup of G generated by H and y. Show that there exists an element $\tilde{\mu} \in \hat{H}'$ that agrees with μ on H. Conclude by induction that there exists a character χ of G that likewise agrees with μ on H. From this and part (b), deduce that for any $g \in G$, there exists a character χ of G such that $\chi(g) \neq 1$. [*Hint*: Given any $t \in S^1$ and $n \geq 1$, one can find $w \in S^1$ such that $w^n = t$.]

(d) Define a map α on G as follows:

$$\alpha : G \to \hat{\hat{G}} = \mathrm{Hom}(\hat{G}, S^1)$$
$$g \mapsto \alpha_g : \chi \mapsto \chi(g) \quad .$$

Show that α is a well-defined injective homomorphism. [*Hint*: Use the previous part.]

(e) Define the map Φ between the group algebras $\mathbf{C}G$ and $\mathbf{C}\hat{G}$ by sending f to its Fourier transform $\hat{f}$. Use part (d) to show that Φ is both $\mathbf{C}$-linear and injective.

(f) Show that any set of distinct characters $\chi_1, \ldots, \chi_r$ of G are linearly independent over $\mathbf{C}$. [*Hint*: Start with a dependency relation of minimal length, and then find a shorter one.]

(g) Let h be an element of $\mathbf{C}\hat{G}$ that does not lie in the image of the map Φ defined above. Show that h must satisfy the equation

$$\sum_{\chi \in \hat{G}} h(\chi)\overline{\hat{f}(\chi)} = 0 \quad .$$

Deduce from this that

$$\sum_{\chi \in \hat{G}} h(\chi)\chi = 0$$

as a function on G. Conclude from this and part (f) that $h(\chi)=0$ for all χ, and from this contradiction that Φ is indeed surjective.

(h) Show that $\dim(\mathbf{C}G)=\dim(\mathbf{C}\hat{G})$. Conclude that the map α defined above is in fact an isomorphism.

14. Let G be a profinite group, or equivalently, a compact, totally disconnected group.

(a) Let $\chi : G \to \mathbf{C}^*$ be a continuous homomorphism. Then show that $\mathrm{Ker}(\chi)$ must contain an open subgroup and that consequently χ must have finite order. [*Hint*: First show that there exists a neighborhood U of $1 \in \mathbf{C}^*$ that contains no nontrivial subgroup of $\mathbf{C}^*$.]

(b) For any $n \geq 1$, let $\rho : G \to \mathrm{GL}_n(\mathbf{C})$ be a continuous homomorphism; that is, a representation of dimension n. Show that $\mathrm{Ker}(\rho)$ must still contain an open subgroup, so that $\rho(G)$ is a finite group.

(c) Fix an algebraic closure $\overline{\mathbf{Q}} \subseteq \mathbf{C}$ of $\mathbf{Q}$, and let $G_{\mathbf{Q}}$ denote the Galois group of $\overline{\mathbf{Q}}$ over $\mathbf{Q}$. For any positive integer m, let μ_m denote the group of mth roots of unity in $\overline{\mathbf{Q}}$. Observe that for any $\sigma \in G_{\mathbf{Q}}$, we have that $\sigma(\mu_m) = \mu_m$. Now choose a rational prime p and set

$$W = \lim_{\substack{\leftarrow \\ n}} \mu_{p^n}.$$

Show that there exists a continuous homomorphism

$$\chi_p : G_{\mathbf{Q}} \to \mathrm{Aut}(W) \cong \mathbf{Z}_p^\times \subseteq \mathbf{Q}_p^\times$$

that, in contrast with the first part of the exercise, is *not* of finite order. (Indeed, one can further imbed $\mathbf{Q}_p$ in $\mathbf{C}$ and thus view χ_p as a complex character on $G_{\mathbf{Q}}$, but this composition is not continuous for the standard complex topology. The character suggested here is called the pth *cyclotomic character.*)

4 The Structure of Arithmetic Fields

This chapter develops the basic structure theory for local and global fields; we follow A. Weil in stressing the topological rather than algebraic perspective, although perhaps less emphatically. Thus the more algebraically inclined will gain new insight into phenomena that have more often been treated in the context of the fraction field of a discrete valuation ring with finite residue field, or a Dedekind domain.

We begin by introducing an essential tool in the topological analysis of locally compact abelian groups and, in particular, of locally compact fields: the so-called module of an automorphism. This leads us to the classification theorem for local fields that appears in the second section, followed by an analysis of the extension of such fields in the third. It is here that we first meet the notion of ramification.

In Section 4.4 we study the more challenging global fields, the analysis of which relies fundamentally on the dense embeddings of a global field F into suitable locally compact fields. Thus the starting point is the classification of the (locally compact) completions of F relative to an absolute value; this is a generalization of Ostrowski's theorem, which says that the completions of $\mathbf{Q}$ are either $\mathbf{R}$ or $\mathbf{Q}_p$, for some prime p. We shall see that the Archimedean ones are indexed by the nonconjugate embeddings of F into $\mathbf{C}$, while the non-Archimedean ones are in bijective correspondence with discrete valuations arising in connection with prime ideals.

In the final section we introduce the decomposition group with its relation to the corresponding local Galois group, further discuss ramification, and conclude with a technical result on global and local bases.

4.1 The Module of an Automorphism

Let G be a locally compact additive group with Haar measure μ and consider a (continuous) automorphism α of G. If X is any Borel subset of G, then so is αX, and thus $\mu \circ \alpha$ is likewise a Haar measure on G. By uniqueness of the Haar measure, it follows that $\mu \circ \alpha = c\mu$ for some positive real constant c, which is then called the *module* of α and denoted $\operatorname{mod}_G(\alpha)$. Thus, by definition, we have

$$\mu(\alpha X) = \mathrm{mod}_G(\alpha)\,\mu(X)$$

for all measurable subsets X of G. Obviously the module is multiplicative in the sense that

$$\mathrm{mod}_G(\alpha\beta) = \mathrm{mod}_G(\alpha)\,\mathrm{mod}_G(\beta)$$

for all automorphisms α and β of G.

As a special case, if k is a locally compact field—what we often refer to more succinctly as a *local field*—and V is any topological vector space over k, then every $a \in k^*$ defines an automorphism of V by left multiplication, and we define $\mathrm{mod}_V(a)$ to be the module of the associated automorphism. We extend mod_V to all of k by defining $\mathrm{mod}_V(0)$ to be 0. In particular, we may define $\mathrm{mod}_k(a)$ for $a \in k$ to be the module of a acting on k itself.

4-1 PROPOSITION. *Let k be a locally compact field with Haar measure μ. Then $\mathrm{mod}_k : k \to \mathbf{R}_+$ is a continuous mapping.*

PROOF. Fix a compact neighborhood X of zero and choose an arbitrary element a lying in k. Note first that by Proposition 1-7, part (iii), $\mu(X) > 0$. Now since μ is outer regular, for every positive ε there is an open set U, $aX \subseteq U$, such that

$$\mu(U) \leq \mu(aX) + \varepsilon \ .$$

Since multiplication is continuous and X is compact, there exists an open neighborhood W of a such that $WX \subseteq U$. But then for all $b \in W$, $bX \subseteq U$, and so

$$\mu(bX) \leq \mu(aX) + \varepsilon$$

whence dividing by $\mu(X)$,

$$\mathrm{mod}_k(b) \leq \mathrm{mod}_k(a) + \mu(X)^{-1}\varepsilon \ .$$

Thus mod_k is at least continuous at zero. Moreover, this shows that for all positive x, the inverse image of $(0,x)$ under mod_k is open. Now clearly

$$\mathrm{mod}_k(a^{-1}) = \mathrm{mod}_k(a)^{-1}$$

and so we have a commutative diagram

$$\begin{array}{ccccc} & k^* & \xrightarrow{\mathrm{mod}_k} & \mathbf{R}_+^\times & \\ (\ )^{-1} & \downarrow & & \downarrow & (\ )^{-1} \\ & k^* & \xrightarrow{\mathrm{mod}_k} & \mathbf{R}_+^\times & \end{array}$$

from which it follows that for all positive x, the inverse image of (x,∞) is likewise open. Hence the inverse image of any open interval is open, and from this we deduce that mod_k is continuous, as claimed. ❑

Since every discrete topological space is trivially locally compact, we can expect serious progress in the classification of locally compact fields only if we exclude this case. (Note in particular that the previous result is trivial for discrete fields.) Accordingly, we shall henceforth address nondiscrete topological fields.

4-2 COROLLARY. *Assume that k is nondiscrete. Let U be any open neighborhood of zero. Then for every positive ε there exists an element $a\in U$ such that* $0<\mathrm{mod}_k(a)<\varepsilon$.

PROOF. The inverse image of $[0,\varepsilon)$ is an open neighborhood of zero. Hence its intersection with U is likewise an open neighborhood of zero. Since k is not discrete, this intersection contains a nonzero element a, which by construction has the required property. ❑

4-3 COROLLARY. *Assume that k is nondiscrete. Then the function* mod_k *is unbounded, and consequently k is not compact.*

PROOF. By the previous corollary, for any positive ε we may find $a\in k^*$ such that $0<\mathrm{mod}_k(a)<\varepsilon$. Hence $\mathrm{mod}_k(a^{-1})\geq\varepsilon^{-1}$, and the assertion follows. ❑

4-4 PROPOSITION. *Let k be as above and let m be a positive number. Define*

$$B_m=\{a\in k:\mathrm{mod}_k(a)\leq m\} \ .$$

Then B_m is compact.

PROOF. Note first that B_m is at least closed by the continuity of mod_k. Let V be a compact neighborhood of zero, and let W be an open neighborhood of zero such that $WV\subseteq V$. Then by the first corollary above there exists an element $r\in W\cap V$ such that $0<\mathrm{mod}_k(r)<1$. We find inductively that $r^n\in V$ for all positive n, whence for any $a\in k$, the sequence $\{r^n a\}$, which lies in the compact set Va, must admit at least one limit point. But clearly $\lim \mathrm{mod}_k(r^n a)=0$, whence by continuity the one and only limit point of this sequence is zero. Since V contains an open neighborhood of zero, it now follows that for all $a\in k$, either a belongs to V or the integer $\nu_a=\inf\{n:r^n a\in V\}$ is finite and positive. In the latter case, clearly

$$r^{\nu_a}a\in V-rV \ . \tag{4.1}$$

We claim that for $a \in B_m - V$, the numbers ν_a are bounded from above by some constant M. Granting this, it follows at once from Eq. 4.1 that the closed subset B_m is contained in the union of compact subsets $V, r^{-1}V, \ldots, r^{-M}V$ and is therefore compact.

PROOF OF CLAIM: Let X be the closure of $V - rV$, which is compact and excludes zero. Set

$$\beta = \inf_{x \in X} \mathrm{mod}_k(x) \quad .$$

Then β is positive, since a continuous function on a compact set achieves its minimum, which in this case cannot be 0. Choose M such that $\mathrm{mod}_k(r)^M < \beta/m$. Then if $a \in B_m - V$, we have

$$\mathrm{mod}_k(r)^M \cdot m \leq \beta \leq \mathrm{mod}_k(r^{\nu_a} a) = \mathrm{mod}_k(r)^{\nu_a} \cdot \mathrm{mod}_k(a) \leq \mathrm{mod}_k(r)^{\nu_a} \cdot m$$

and since $0 < \mathrm{mod}_k(r) < 1$, we must have $\nu_a \leq M$. This completes the proof. ❑

4-5 COROLLARY. *For $a \in k$, $\lim_{n\to\infty} a^n = 0$ if and only if $\mathrm{mod}_k(a) < 1$.*

PROOF. If $\mathrm{mod}_k(a) < 1$, then the elements a^n lie in the compact set B_1, and therefore the sequence $\{a^n\}$ converges. By continuity, the limit has module zero and is therefore itself zero. The converse is obvious. ❑

4-6 COROLLARY. *Let l be a discrete field contained in k. Then for all $a \in l^*$, $\mathrm{mod}_k(a) = 1$. Moreover, l is finite.*

PROOF. Suppose that $a \in l^*$ but $\mathrm{mod}_k(a) < 1$. Then the sequence $\{a^n\}_{n>0}$ lies in l, which, according to the previous corollary, is therefore not discrete—a contradiction. If $\mathrm{mod}_k(a) > 1$, the same argument applies to a^{-1}. This establishes the first assertion and shows moreover that $l \subseteq B_1$. But a discrete subset of a compact set must be finite. ❑

4-7 PROPOSITION. *The sets B_m constitute a local base at zero for the topology of k.*

PROOF. Recall first that for a locally compact Hausdorff space, we at least know that the compact neighborhoods of a given point constitute a local base. On any compact neighborhood V of zero in k, mod_k is bounded, say by m. Then certainly $V \subseteq B_m$, and X, the complement of the interior of V in B_m, is likewise compact and excludes zero. As above, set

$$\beta = \inf_{x\in X} \operatorname{mod}_k(x) > 0 \quad .$$

Choosing γ in $\mathbf{R}$ such that $0<\gamma<\beta$, we have $B_\gamma \subseteq V$, and this completes the proof. ❑

4-8 PROPOSITION. *The function* mod_k *induces an open homomorphism of* $k^\times$ *onto a closed subgroup* Γ *of* $\mathbf{R}_+^\times$.

PROOF. Let x be the limit of a sequence $\{\operatorname{mod}_k(a_j)\}_j$ where each $a_j \in k$. Then since mod_k is bounded on this sequence, eventually the a_j fall into a compact ball B_m for some m. Hence x lies in the closure of the continuous image of a compact set, which must itself be closed. It follows that in fact $x \in \operatorname{mod}_k(B_m)$, whence $\operatorname{mod}_k(k)$ is closed. Accordingly Γ is closed in the usual induced topology on $\mathbf{R}_+^\times$.

We next establish that mod_k is open on $k^\times$. Let U denote the kernel of the restricted map, so that we have a short exact sequence of commutative groups

$$1 \to U \to k^\times \to \Gamma \to 1 \quad .$$

Let V be an open subset of $k^\times$ and let $\{x_j\}$ be any sequence in Γ converging to some $x \in \operatorname{mod}_k(V)$. Say $x = \operatorname{mod}_k(a)$ for some $a \in V$. The sequence $\{x_j\}$ pulls back via mod_k to a sequence $\{a_j\}$ in the unit group $k^\times$, and so as above, eventually the points fall into one of the compact balls B_m. Therefore some subsequence $\{a'_j\}$ of the sequence $\{a_j\}$ converges, say, to $\alpha \in k^\times$. By continuity, $\operatorname{mod}_k(\alpha) = x$ also, whence by group theory $\alpha \in aU \subseteq VU$. Since VU is open, eventually the points of $\{a'_j\}$ must lie in the product of these two subsets. But by construction, $\operatorname{mod}_k(VU) = \operatorname{mod}_k(V)$, showing that the subsequence $\{\operatorname{mod}_k(a'_j)\}$ of the original sequence $\{x_j\}$—and hence the entire sequence—eventually falls into $\operatorname{mod}_k(V)$. The image of V under mod_k is therefore open, as claimed. ❑

4-9 THEOREM. *Let k be a locally compact, nondiscrete topological field with Haar measure μ. Then:*

(i) *There exists a positive constant $A \geq 1$ such that*

$$\operatorname{mod}_k(a+b) \leq A \cdot \sup\{\operatorname{mod}_k(a), \operatorname{mod}_k(b)\} \;\; \forall a,b \in k \quad . \tag{4.2}$$

(ii) *If $A=1$, then $\operatorname{mod}_k(k^*)$ is discrete.*

PROOF. Define A by the formula

$$A = \sup_{b\in B_1}\{\operatorname{mod}_k(1+b)\} \quad .$$

Since the supremum is taken over a compact set (a translate of B_1), A is indeed finite and clearly greater than or equal to 1. Moreover, taking $a=1$ in the inequality 4.2, we see that the number defined by this formula is clearly the smallest possible value for which the stated inequality can hold.

To show now that inequality 4.2 holds for all a and b, it clearly suffices to consider the case that either a or b is not zero. So assume that a is not zero and that $\mathrm{mod}_k(b) \le \mathrm{mod}_k(a)$. (Otherwise, b is likewise nonzero, and we can switch the roles of a and b.) Then setting $c=a^{-1}b$, we have $\mathrm{mod}_k(c) \le 1$ and $a+b=a(1+c)$. By construction, $\mathrm{mod}_k(1+c) \le A$, and therefore

$$\begin{aligned}\mathrm{mod}_k(a+b) &= \mathrm{mod}_k(a)\,\mathrm{mod}_k(1+c)\\ &\le A\cdot\mathrm{mod}_k(a)\\ &= A\cdot\sup\{\mathrm{mod}_k(a),\mathrm{mod}_k(b)\}\end{aligned}$$

as claimed in part (i).

To prove (ii), suppose that $A=1$. Let U denote the interior of B_1, which obviously contains 0. Then mod_k maps $1+U$ into an open subset of Γ that contains 1 but is itself contained in $[0,1]$. This means that $\mathrm{mod}_k(1+U)$ is the intersection of an open subset of $\mathbf{R}$ with Γ, and, in particular, that there is an open interval I containing 1 whose intersection with Γ is contained in $[0,1]$. However, 1 is an accumulation point from the left in Γ if and only if it is also an accumulation point from the right, since $\mathrm{mod}_k(a^{-1}) = \mathrm{mod}_k(a)^{-1}$ for all $a \ne 0$, and so such an interval I cannot exist unless 1 is *not* an accumulation point of Γ. But then the set consisting of 1 alone is open in Γ, which is to say that Γ enjoys the discrete topology, as claimed. ❑

DEFINITION. If k satisfies the inequality of part (i) with $A=1$, then we say that k (or mod_k) is *ultrametric*. In this case,

$$\mathrm{mod}_k(a+b) \le \sup\{\mathrm{mod}_k(a),\mathrm{mod}_k(b)\} \quad \forall a,b \in k$$

and we call this the *ultrametric inequality*.

Via an easy induction, the ultrametric inequality implies that $\mathrm{mod}_k(n\cdot 1_k) \le \mathrm{mod}_k(1_k) = 1$ for all $n \in \mathbf{N}$, so that for an ultrametric field mod_k is bounded by 1 on the prime ring. We shall establish the converse, and more, shortly.

The following propositions establish some properties of mod_k that depend on the inequality 4.2 of the previous theorem. The first holds more generally for *any* strictly multiplicative function.

4-10 PROPOSITION. *Let $F:\mathbf{N}\to\mathbf{R}_+$ be a strictly multiplicative function [i.e., for all natural numbers m and n, $F(mn)=F(m)F(n)$], and assume that there exists some constant A such that*

$$F(m+n) \leq A \cdot \sup\{F(m), F(n)\}$$

for all $m, n \in \mathbf{N}$. *Then either* (i) $F(m) \leq 1$ *for all* m, *or* (ii) $F(m) = m^{\lambda}$ *for some positive constant* λ.

PROOF. We note first that since F is strictly multiplicative, the idempotents 0 and 1 must map onto idempotents, which is to say 0 and 1. Moreover, from the identities $F(0) = F(0 \cdot n) = F(0) \cdot F(n)$ and $F(n) = F(1 \cdot n) = F(1) \cdot F(n)$ we deduce that if F is not constant, then $F(0)$ must be 0 and $F(1)$ must be 1.

Define an auxiliary function $f: \mathbf{N} \to \mathbf{R}_+$ by

$$f(m) = \begin{cases} 0 & \text{if } F(m) = 0 \\ \log F(m) & \text{otherwise.} \end{cases}$$

We shall show that for $m \geq 2$, $f(m) = \lambda \log m$ for some constant λ. Let $a = \log A$. Then we have the following relations for all m, n, and nonzero j:

$$f(m^j) = j \cdot f(m)$$
$$f(mn) \leq f(m) + f(n)$$
$$f(m+n) \leq a + \sup\{f(m), f(n)\}$$

The middle relation is, of course, an equality, provided that neither m nor n is zero. The last extends inductively to

$$f(\sum_{i=0}^{r} m_i) \leq ra + \sup_i\{f(m_i)\} \quad .$$

Now assume that $m, n \geq 2$, and let $b = \sup\{f(0), \ldots, f(n-1)\}$. Express m in base n as follows:

$$m = \sum_{i=0}^{r} d_i n^i \qquad (0 \leq d_i < n,\ i = 0, \ldots, r) \quad .$$

We assume in particular that d_r is nonzero, whence $n^r \leq m$. Then by the general properties above, $f(m) \leq ra + b + rf(n)$, whence the further inequality

$$\frac{f(m)}{\log m} \leq \frac{a + f(n)}{\log n} + \frac{b}{\log m} \quad .$$

Replacing m by m^j and taking j to infinity yields

$$\frac{f(m)}{\log m} \leq \frac{a + f(n)}{\log n} \quad .$$

Repeating this argument for n in this last inequality yields finally

$$\frac{f(m)}{\log m} \leq \frac{f(n)}{\log n} \quad .$$

whence by symmetry, we deduce that $f(m)/\log m$ is a constant for $m \geq 2$. Hence for such m, $f(m) = \lambda \log m$ for some constant λ, as claimed above.

If λ is 0, then clearly alternative (i) holds for $m \geq 2$, and the remaining cases ($m = 0, 1$) are covered by our preliminary analysis.

If λ is positive, then alternative (ii) holds for $m \geq 2$, and it only remains to check $m < 2$. But in this case F is not constant, and once again our preliminary analysis yields the desired result. ❑

Note that a function F on an arbitrary field k induces a function on **N** (or even **Z**) by defining $F(m) = F(m \cdot 1_k)$. In particular, the function mod_k induces a strictly multiplicative function on **N**.

4-11 PROPOSITION. *If* mod_k *is bounded on the prime ring of k (that is, if the induced map on* **N** *is bounded), then in fact* $\text{mod}_k \leq 1$ *on the prime ring, and moreover, k is ultrametric.*

PROOF. Since $\text{mod}_k(m^j) = \text{mod}_k(m)^j$, the induced map cannot be bounded unless its values lie in $[0,1]$. It remains to show that k is ultrametric. Let $N = 2^n$. Then by successively splitting the summation

$$\sum_{j=1}^{N} a_j$$

into two summations, each involving half as many terms, we find that

$$\text{mod}_k\Big(\sum_{j=1}^{N} a_j\Big) \leq A^n \sup_j \{\text{mod}_k(a_j)\}$$

which clearly implies the following more general inequality for arbitrary N:

$$\text{mod}_k\Big(\sum_{j=1}^{N} a_j\Big) \leq A^{\lceil \log_2(N) \rceil} \sup_j \{\text{mod}_k(a_j)\} \quad .$$

Thus

$$\text{mod}_k(a+b)^{2^n} \leq A^{n+1} \sup_{0 \leq j \leq 2^n} \Big\{\text{mod}_k\Big(\binom{2^n}{j}\Big) \text{mod}_k(a)^j \, \text{mod}_k(b)^{2^n - j}\Big\} \quad .$$

Without loss of generality, assume that $\operatorname{mod}_k(a) \leq \operatorname{mod}_k(b)$. Then since mod_k is bounded by 1 on the prime ring, the previous inequality simplifies to

$$\operatorname{mod}_k(a+b)^{2^n} \leq A^{n+1} \operatorname{mod}_k(a)^{2^n} .$$

Taking logarithms, dividing by 2^n, and letting n tend to infinity shows that $\operatorname{mod}_k(a+b) \leq \operatorname{mod}_k(a)$, and thus k is ultrametric, as claimed. ❑

4.2 The Classification of Locally Compact Fields

The main point of this section is the following classification theorem.

4-12 THEOREM. *Let k be any nondiscrete locally compact field. Then:*

(i) *If* $\operatorname{char}(k)=0$, *k is* $\mathbf{R}$ *or* $\mathbf{C}$ *or a finite extension of* $\mathbf{Q}_p$.

(ii) *If* $\operatorname{char}(k)=p>0$, *then k is ultrametric and isomorphic to the field of formal power series in one variable over a finite field (i.e., the quotient field of* $\mathbf{F}_q[[t]]$ *for some finite field* $\mathbf{F}_q$ *and indeterminate t).*

We begin with some preliminary results on topological vector spaces.

Topological Vector Spaces over Nondiscrete Locally Compact Fields

Let V be a topological vector space over a nondiscrete locally compact field k, and let W be a finite-dimensional subspace of V of dimension n. Assume further that W has basis $w_1, \ldots, w_n$. Consider the map

$$\begin{array}{ccc} k^n & \xrightarrow{\varphi} & W \\ (a_j) & \mapsto & \sum a_j w_j \end{array} .$$

Clearly φ is a sum of continuous functions, from which one deduces at once that φ is a continuous isomorphism of topological vector spaces.

4-13 PROPOSITION. Given *k, V, W, and φ as above, the following assertions hold:*

(i) *Let U be any open neighborhood of zero in V. Then* $W \cap U \neq \{0\}$.

(ii) *The mapping φ is a homeomorphism. Consequently W admits precisely one structure as a topological vector space over k.*

(iii) *W is closed and locally compact.*

(iv) *If V is itself locally compact, then V is finite-dimensional over k, and $\mathrm{mod}_V(a)=\mathrm{mod}_k(a)^{\dim V}$ for all $a\in V$.*

PROOF. (i) $W\cap U$ must contain something other than zero, else via φ^{-1} the zero vector would constitute an open subset of k^n, contradicting the assumption that k is not discrete.

(ii) We need only show that φ is an open mapping. Since according to Proposition 4-7, the sets

$$B_t=\{a\in k:\mathrm{mod}_k(a)\le t\}\quad (t>0)$$

constitute a local base at zero for k, it suffices to show that for all positive t, $\varphi(B_t^n)$ contains a neighborhood of $0\in W$. We introduce an auxiliary map

$$\begin{array}{ccc} k^n & \overset{\psi}{\to} & \mathbf{R}_+^n \\ (a_j) & \mapsto & (\mathrm{mod}_k(a_j))_{j=1,\dots,n} \end{array}$$

which is continuous by Proposition 4-1. Define subsets A of k^n and X of $\mathbf{R}_+^n$, respectively, by

$$A=\{(a_j)\in k^n\colon \sup_j\,(\mathrm{mod}_k(a_j))=1\}$$

and

$$X=\bigcup_i\{(x_j)\in\mathbf{R}_+^n\colon x_i=1,\ x_j\le 1 \text{ for } j\ne i\}\quad .$$

Clearly neither set contains zero. Note, moreover, that X is closed in $\mathbf{R}_+^n$, and therefore A, which is precisely $\psi^{-1}(X)$, is likewise closed in k^n. Furthermore, A is a subset of the compact set B_1^n and therefore itself compact.

Now consider $\varphi(A)$, a compact subset of V, which also does not contain zero. Since scalar multiplication is a continuous map from $k\times V$ to V, the inverse image of $V-\varphi(A)$ contains an open neighborhood of $(0_k,0_V)$. Again, since the sets B_t constitute a local base at zero for k, it follows that there exists an open neighborhood U of zero and an $\varepsilon>0$ such that $B_\varepsilon U\cap\varphi(A)=\varnothing$. This is to say that if $y\in k$ with $\mathrm{mod}_k y\le\varepsilon$, then $yU\cap\varphi(A)=\varnothing$.

Fix $t>0$ and choose $a\in k$ such that $0<\mathrm{mod}_k(a)\le\varepsilon t$. (Such a exist according to Corollary 4-2.) By part (i), the set $(W\cap aU)-\{0\}$ is nonempty; suppose that $w=\sum a_jw_j$ lies therein. Let h be the index such that $\mathrm{mod}_k(a_h)$ is maximal and hence positive. Finally, define the following parameters:

$$b_j = a_h^{-1} a_j \quad (j = 1, \dots, n)$$
$$z = a_h^{-1} w$$

Since (b_j) lies in A, z lies in $\varphi(A)$. Since w lies in aU, z lies in yU with $y = a_h^{-1}a$. By definition of U and ε we must have that $\mathrm{mod}_k(y) > \varepsilon$. Therefore,

$$\mathrm{mod}_k(a_h) < \varepsilon^{-1} \mathrm{mod}_k(a) \le t \ .$$

This implies that $(a_j) \in B_t^n$ and that $w \in \varphi(B_t^n)$. We conclude that

$$W \cap aU \subseteq \varphi(B_t^n)$$

whence $\varphi(B_t^n)$ indeed contains a neighborhood of 0 in W, and therefore φ is open.

(iii) Clearly W is locally compact by part (ii). Suppose that z lies in the closure of W but not in W itself. Then again by part (ii), we have a homeomorphism of k^{n+1} onto $\langle W, z \rangle$, the subspace generated by W and z, which maps the closed subspace $k^n \times \{0\}$ onto W. It follows that W itself is closed in $\langle W, z \rangle$, whence $z \in W$—a contradiction. Thus W is closed in V, as claimed.

(iv) Assuming for the moment that V is indeed finite-dimensional over k, in light of part (ii) it suffices to prove the formula for $\mathrm{mod}_V(a)$ for $V = k^n$. But by Fubini's theorem, the effect of left multiplication by a on the measure of a measurable subset of k^n may be computed iteratively over each of the coordinates, and from this we deduce immediately that $\mathrm{mod}_V(a) = \mathrm{mod}_k(a)^n$, as claimed.

It remains to show that a locally compact topological vector space V is indeed of finite dimension over k. Let there be given $a \in k$ such that $0 < \mathrm{mod}_k(a) < 1$. Then according to Corollary 4-5, we have that $\lim a^n = 0$, whence $\mathrm{mod}_V(a) < 1$ also. (Note that this holds for *any* nontrivial locally compact topological vector space V over k: by continuity of multiplication, for any compact $K \subseteq V$, $a^n K$ eventually falls into neighborhoods of 0 of arbitrarily small measure.) Let W be a finite-dimensional subspace of V, which is therefore closed by part (iii), and consider the quotient space $V' = V/W$. By devissage (see Exercise 3),

$$\mathrm{mod}_V(a) = \mathrm{mod}_W(a)\, \mathrm{mod}_{V'}(a) = \mathrm{mod}_k(a)^{\dim W} \mathrm{mod}_{V'}(a)$$

and since $\mathrm{mod}_{V'}(a) \le 1$ with equality if and only if $V' = \{0\}$, we have $\mathrm{mod}_{V'}(a) \le \mathrm{mod}_k(a)^{\dim W}$. But this upper bound is valid for all finite-dimensional subspaces W, hence $\dim V$ must be finite or else $\mathrm{mod}_V(a)$ would be 0—a contradiction that completes the proof. ❑

Preliminary Analysis for the Main Theorem

We develop some general statements about mod_k that will be needed in the proof of the main theorem. In fact this analysis allows us to settle the case of characteristic zero in short order.

Recall from the previous section that we define mod_k for **N** by the formula $\text{mod}_k(m)=\text{mod}_k(m\cdot 1_k)$ and that according to Proposition 4-10, either

(1) $\text{mod}_k(m)\leq 1$ for all m (equivalently, k is ultrametric by Proposition 4-11), or

(2) there is a positive constant λ such that $\text{mod}_k(m)=m^\lambda$ for all m.

Assume first that alternative (1) holds, which is always the case for k of positive characteristic, since then mod_k is clearly bounded on the prime ring of k. We then have

$$\{m\cdot 1_k : m\in\mathbf{N}\}\subseteq B_1$$

and since B_1 is compact, there exists at least one limit point a. For every positive ε there are infinitely many m such that $\text{mod}_k(m\cdot 1_k-a)\leq\varepsilon$. Let m and m' be two such integers with $m<m'$. By the ultrametric inequality,

$$\text{mod}_k((m'-m)\cdot 1_k)=\text{mod}_k(m'\cdot 1_k - m\cdot 1_k)\leq\varepsilon\ .$$

In particular, there exists $n\geq 1$ such that $\text{mod}_k(n)<1$. Let p be the smallest positive integer for which this inequality holds. Since mod_k is multiplicative, p must be prime (see the proof of Theorem 4-30), and by induction, moreover, $\text{mod}_k(mp)<1$ for every $m\in\mathbf{N}$. Let j be a positive integer less than p. From the identity

$$j=(j+mp)-mp$$

it follows from the minimality of p and again from the ultrametric inequality that

$$\text{mod}_k(j+mp)=1\ .$$

Thus if n is any positive integer prime to p, then $\text{mod}_k(n)=1$, and in particular, p is the *unique* prime at which mod_k is less than 1. This leads us to two possibilities:

(a) Suppose that $\text{char}(k)>0$. In this case $\text{mod}_k(\text{char}(k))=0$, and according to the analysis above, p is in fact equal to $\text{char}(k)$.

(b) Suppose, still under alternative (1), that char(k)=0. Then $\mathrm{mod}_k(p)$ is not zero, and we may write $\mathrm{mod}_k(p)=p^{-t}$ for some positive t. Expressing arbitrary n as mp^r with m prime to p, we see at once that

$$\mathrm{mod}_k(n) = |n|_p^t$$

where $|\cdot|_p$ is the p-norm on $\mathbf{Q}$. [For nonzero c, the p-norm is defined as follows: express c in the form $p^m(a/b)$ where a and b are integers relatively prime to p; then $|c|_p=p^{-m}$.]

Let $|\cdot|_\infty$ denote the usual norm on $\mathbf{R}$. It follows from case (b) that in characteristic zero, under either alternative (1) or (2), we have that for all natural numbers n,

$$\mathrm{mod}_k(n) = |n|_v^t \tag{4.3}$$

where v is the prime p described above if alternative (1) holds and p is ∞ if alternative (2) holds. Thus in this case the module has a uniform characterization. Indeed, Eq. 4.3 is the key to the analysis in characteristic zero, as we shall see in the following subsection.

REMARK. Note finally that if $\mathrm{mod}_k(p)<1$ for some positive rational prime p, then either (a) holds, or (b) holds with $v=p$. In either case, k is ultrametric.

Proof of the Main Theorem in Characteristic Zero

We now dispense with the case char(k)=0. The isomorphism of algebras

$$\begin{array}{ccc} \mathbf{Z} & \to & \mathbf{Z}\cdot 1_k \\ n & \mapsto & n\cdot 1_k \end{array}$$

extends to an isomorphism $\mathbf{Q}\to 1_k\cdot\mathbf{Q}\subseteq k$, which we regard as an identification. By Eq. 4.3, mod_k induces the function $x\mapsto|x|_v^t$ on $\mathbf{Q}$. Since the sets B_t constitute a local base at 0 in k, the topological structure of $\mathbf{Q}$ induced by k is identical to that induced by the distance function $|x-y|_v$. Hence in view of k's local compactness, the closure $\hat{\mathbf{Q}}$ of $\mathbf{Q}$ in k is precisely the completion $\mathbf{Q}_v$ of $\mathbf{Q}$ relative to the metric v; that is, $\hat{\mathbf{Q}}\cong\mathbf{Q}_v$ (as locally compact fields). By Proposition 4-13, part (iv), k is finite-dimensional over $\mathbf{Q}_v$, so that if $v=\infty$, k is a finite field extension of $\mathbf{R}$, and hence is either $\mathbf{R}$ or $\mathbf{C}$. Otherwise, if $v=p$, then k is a finite-dimensional extension of the p-adic field $\mathbf{Q}_p$. This completes the proof of assertion (i) of the main theorem. ❑

The bulk of the proof of assertion (ii) of the main theorem is in the analysis of the local ring associated with a locally compact ultrametric field.

The Local Ring of an Ultrametric Field and Its Residue Field

Assume that k is ultrametric. Recall in particular (Proposition 4-9) that Γ, the image of k^* under mod_k, is discrete in $\mathbf{R}_+^\times$. We define the following subsets of k:

$$\begin{aligned} A &= \{x \in k \mid \text{mod}_k(x) \le 1\} \\ A^\times &= \{x \in k \mid \text{mod}_k(x) = 1\} \\ P &= \{x \in k \mid \text{mod}_k(x) < 1\} \end{aligned}$$

We begin with an analysis of the major structural features of A, P, and A/P.

4-14 LEMMA. *A is the unique maximal compact subring of k, and $A^\times$ (as defined above) is the group of units of A.*

PROOF. Note first that $A = B_1$ is compact, whence its closed subset $A^\times$ is likewise compact. By the ultrametric inequality and the multiplicativity of mod_k, A is clearly a ring with unit group $A^\times$, as claimed. If S is any relatively compact multiplicative subset of k, then $a \in S$ implies that the sequence $\{a^n\}$ has an accumulation point in S, and so $\text{mod}_k(a) \le 1$. Thus $S \subseteq A$, and A is indeed maximal, as required. ❑

Recall that a *local ring* is an integral domain that has a unique maximal ideal. Clearly every element lying outside of this maximal ideal is a unit. A *discrete valuation ring* is a principal ideal domain having a unique prime ideal; it is in particular a local ring. The unique prime ideal of a discrete valuation ring R takes the form $R\pi$, where π, the unique irreducible element of R (up to associates), is called the *uniformizing parameter* of R.

4-15 LEMMA. *A is a discrete valuation ring, and hence a local ring, with unique maximal ideal $P = A\pi$, where the uniformizing parameter π is given as any element in k^* such that $\gamma = \text{mod}_k(\pi)$ is the maximal element of Γ less than 1. Moreover, the residue field A/P is finite.*

PROOF. By the ultrametric inequality, P is obviously an ideal of A, and since $P = A - A^\times$, it is, moreover, open and the unique maximal ideal of A. Note also that our description of $\pi \in k^*$ is sensible, since Γ is discrete, and that π is necessarily irreducible in A. One shows easily that γ generates Γ, so that we have a short exact sequence of groups

$$1 \to A^{\times} \to k^* \overset{\text{mod}_k}{\to} \Gamma \to 1$$

whence every element in $a \in k^*$ is expressible uniquely in the form $u\pi^n$ for some $u \in A^{\times}$ and integer n, called the *order* of a and denoted $\text{ord}_k(a)$. (For convenience, we set $\text{ord}_k(0) = +\infty$.) Consequently every proper ideal of A is generated by its element of minimal order and thus of the form $\pi^n A$ for some positive integer n. Hence A is *ipso facto* a discrete valuation ring with unique maximal ideal $P = A\pi$. Since P is open and A is compact, the residue ring A/P is discrete, compact, and hence finite. This complete the proof. ❑

4-16 COROLLARY. *Every automorphism σ of k (as a topological field) maps A to A and P to P; hence it induces an automorphism $\bar{\sigma}$ on A/P.*

PROOF. A must map onto itself by virtue of its description as the maximal compact subring of k, and since a (unital) ring homomorphism maps units to units, $P = A - A^{\times}$ likewise maps onto itself. ❑

Henceforth we put $q = \text{Card}(A/P)$. If $\text{mod}_k(p) < 1$ for some rational prime p, then as observed in the remark above, k is ultrametric, and the present discussion applies. Also, by definition $p \cdot 1_k \in P$, so that the characteristic of the residue field A/P must be p, and $q = p^r$ for some positive integer r. Since A is compact, and therefore of finite measure, and A is the disjoint union of q additive translates of $P = \pi A$, $\mu(A) = q\mu(\pi A)$, so that $\text{mod}_k(\pi) = q^{-1}$. We call q the *module* of k. Thus

$$\text{mod}_k(a) = q^{-\text{ord}_k(a)} \quad (a \in k^*) \ . \tag{4.4}$$

4-17 PROPOSITION. *Assume that k is locally compact and that* $\text{mod}_k(p) < 1$ *for some prime p. Then the following assertions hold:*

(i) *Let $\{a_j\}_{j \geq 0}$ be a sequence in k such that* $\lim a_j = 0$. *Then the series*

$$\sum_{j=0}^{\infty} a_j$$

converges in k.

(ii) *Let $\{a_j\}$ be a fixed set of coset representatives for A/P that includes* 0 *and let $a \in k^*$ have order n. Then a is expressible uniquely in the form*

$$a = \sum_{j=n}^{\infty} a_j \pi^j \tag{4.5}$$

with $a_n \neq 0$.

PROOF. (i) Since mod_k is continuous, we must have also that $\lim \mathrm{mod}_k(a_j) = 0$. Consider the sequence of partial summations

$$S_n = \sum_{j=0}^{n} a_j \quad .$$

Since k is ultrametric, for $m<n$,

$$\mathrm{mod}(S_n - S_m) \leq \sup_{m<j\leq n} \mathrm{mod}_k(a_j) \leq \sup_{m<j} \mathrm{mod}_k(a_j)$$

and the bound can be made arbitrarily small. We see that the S_n must fall into a compact subset of k and there accumulate to a unique limit point.

(ii) Since the a_j are chosen from a fixed finite set, the numbers $\mathrm{mod}_k(a_j\pi^j)$ converge to zero, and hence so do the field elements $a_j\pi^j$. By part (i), a series of the given form always converges. Next consider the possibility that

$$\sum_{j=0}^{\infty} a_j \pi^j = 0$$

but not all the a_j are zero. If j_0 is the first index such that $a_{j_0} \neq 0$, then

$$\pi^{j_0} = a_{j_0}^{-1} \sum_{j=j_0+1}^{\infty} a_j \pi^j$$

(each a_j except 0 is a unit), which is impossible, since mod_k applied to the left is q^{-j_0}, but mod_k applied to the right is bounded by $q^{-(j_0+1)}$. It follows that any representation of the form given in Eq. 4.5 is unique. Finally, given $a \in k^*$, after multiplication by π^{-n} we may assume that $a \in A^\times$. We may then inductively choose a_j such that

$$a \equiv \sum_{j=0}^{n-1} a_j \pi^j \pmod{P^n} \quad .$$

Note that $a_0 \neq 0$ because $a \notin P$. Thus

$$\mathrm{mod}_k(a - \sum_{j=0}^{n-1} a_j \pi^j) \leq q^{-n}$$

and as $n \to \infty$, the partial sums converge to a. This completes the proof. ❑

Roots of Unity in k

We continue to assume that $\text{mod}_k(p)<1$ for some rational prime p (with all notation as in the preceding subsection). In particular, this condition holds if $\text{char}(k)=p$. We examine a special subgroup of k^* that is simultaneously a transversal for $(A/P)^*$. From this we shall easily deduce part (ii) of the classification theorem (Theorem 4-12).

We begin with a technical lemma. Recall that q, the module of k, is also the order of the finite residue field A/P and that $q=p^r$ for some positive integer r.

4-18 LEMMA. *Let $a\in A^\times$ and define a sequence in A as follows:*

$$a_0 = a$$
$$a_n = a^{q^n} - a^{q^{n-1}} \quad (n \geq 1)$$

Then $\{a_n\}$ converges to zero, and hence $\lim_{n\to\infty} a^{q^n}$ exists.

PROOF. Since by assumption $p\cdot 1_k\in P$, an easy induction shows that

$$(1+P)^{p^n} \subseteq 1+P^{n+1} \quad .$$

Now $(A/P)^*$ has order $q-1$, so clearly $a^{q-1}\in 1+P$, and from the inclusion above it follows that $a^{(q-1)q^n} \in 1+P^{rn+1}$. Therefore,

$$a_{n+1} = a^{q^{n+1}} - a^{q^n} = a^{q^n}(a^{(q-1)q^n} - 1) \in P^{rn+1}$$

whence $\lim_{n\to\infty} \text{mod}_k(a_n) = 0$. Thus by continuity $\lim_{n\to\infty} a_n = 0$, as claimed. The second statement follows from Proposition 4-17, part (i), since the nth partial sum of the series $\sum a_j$ is precisely a^{q^n}. ❑

According to the lemma, we can sensibly define

$$\omega(a) = \lim_{n\to\infty} a^{q^n}$$

for $a\in A^\times$. The definition also makes sense for $a\in P$ (where the limit is 0) and hence for all of A. Moreover,

$$\omega(ab) = \omega(a)\omega(b)$$

for all $a,b\in A$, and in particular, $\omega(a^n)=\omega(a)^n$ for all integers n and $a\in A^\times$.

Recalling that $(1+P)^{p^n} \subseteq 1+P^{n+1}$, we see that $\omega(a)=1$ if $a \equiv 1 \pmod{P}$. Conversely, if $\omega(a)=1$, then eventually $(a-1)^{q^n} = a^{q^n} - 1 \in P$, and so $a \equiv 1 \pmod{P}$. Thus the inverse image of zero under ω is P, while the inverse image of 1 is precisely $1+P$. Note, too, that since $a^{q-1} \in 1+P$ for all $a \in A^\times$, $\omega(a)^{q-1}=1$. Choose an element $a_1 \in A^\times$ whose projection generates $(A/P)^*$ and put $\mu_1 = \omega(a_1)$. We claim that μ_1 generates a cyclic group of order $q-1$ in $A^\times$.

Proof of Claim. For any integer n, we have the following chain of equivalences:

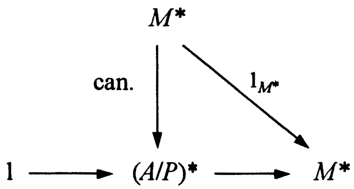
$$\begin{aligned} \mu_1^n = 1 &\Leftrightarrow \omega(a_1^n) = 1 \\ &\Leftrightarrow a_1^n \in 1+P \\ &\Leftrightarrow n \equiv 0 \pmod{q-1} \end{aligned}$$

Clearly this can hold if and only if μ_1 generates cyclic group of order $q-1$. ❑

Define M^* to be the group of roots of unity in k of order prime to p. The upshot of this discussion is that ω induces an injective homomorphism of groups $(A/P)^* \to M^*$. This induced map turns out to be an isomorphism.

4-19 Proposition. *For every $a \in M^*$, $\omega(a)=a$. Hence the factorization of ω through the canonical projection onto $(A/P)^*$ induces an isomorphism of groups $M^* \cong (A/P)^*$. Thus $M = M^* \cup \{0\}$ constitutes a complete set of coset representatives for A/P, and the polynomial $x^{q-1}-1$ splits in k.*

Proof. Let $a \in M^*$ be of order n, and let N be the order of q in $\mathbf{Z}/n\mathbf{Z}$, so that $q^N \equiv 1 \pmod{n}$. Then $a^{q^{jN}} = a$ for all $j \geq 0$, and consequently $\omega(a)=a$. Since M^* is a torsion group, this suffices to establish the first statement. The balance of the proposition is easily deduced from the following commutative diagram:



❑

In the case of positive characteristic, $M = M^* \cup \{0\}$ turns out to be much more than a commutative monoid, and this is the key to part (ii) of the classification theorem.

4-20 Proposition. *Assume that k is of positive characteristic p. Then M is the algebraic closure of $\mathbf{F}_p$ in k.*

PROOF. Let $\overline{M}$ be the algebraic closure of $\mathbf{F}_p$ in k. We must show that every nonzero element $a \in \overline{M}$ is a root of unity of order prime to p. Certainly a lies in some finite extension of $\mathbf{F}_p$, so that $a^{p^m-1} = 1$ for some $m \geq 1$. Hence the order of a has no factor of p, and $a \in M$, as required. ❑

Combining this result with the representation of k by power series in the uniformizing parameter π [Proposition 4-17, part (ii)] yields the following result.

4-21 PROPOSITION. *Assume that k is locally compact with* $\mathrm{mod}_k(p) < 1$ *for some rational prime p. Then*

(i) *Every element of P^n ($n \in \mathbf{Z}$) is uniquely expressible as*

$$\sum_{j \geq n}^{\infty} a_j \pi^j \quad (a_j \in M) \ .$$

(ii) *$\langle M,+\rangle$ is a subgroup of $\langle k,+\rangle$ (and hence M is a field) if and only if* $\mathrm{char}(k)$ *is positive.*

PROOF. We need only demonstrate (ii) in the forward direction. But this follows at once from the existence of an injection of M into the finite set A/P: if M is closed under addition, it must have torsion, whence k has positive characteristic. ❑

Proof of the Main Theorem in Positive Characteristic

We consider the second statement of Theorem 4-12, the case $\mathrm{char}(k)=p>0$, to which the previous discussion applies. By the preceding proposition, every element of k can be expressed uniquely as a power series in π with coefficients in M (possibly involving finitely many terms with negative exponent). If k is of positive characteristic, then M is a field and the assignment $\pi \mapsto x$ induces an isomorphism from k to $M((x))$, the field of formal power series in the indeterminate x with coefficients in M. This completes the proof. ❑

4.3 Extensions of Local Fields

Returning to the more general case of a nondiscrete locally compact field k with $\mathrm{mod}_k(p)<1$, with no assumption on the characteristic of k, we now develop some fundamental results on finite extensions. Accordingly, let k_1/k be an extension of k of degree n. Recall that k_1 has a unique topology as a topological vector space over k, in which category it is isomorphic to k^n. It follows that k_1 is also nondiscrete and that any k-linear map of k_1 onto itself preserves this topology, which is to say that $\mathrm{Aut}(k_1/k) \cong \mathrm{Aut}_{\mathrm{top}}(k_1/k)$.

SPECIAL CONVENTION. For this section we adopt the following convention: if X denotes any structure or invariant defined with respect to k, then X_1 denotes that same structure or invariant defined with respect to k_1. Thus A and A_1 are, in particular, the local rings associated with the fields k and k_1, respectively.

Ramification Index and Residual Degree

We shall now see how the finite extension k_1/k of a local field k gives rise to a finite extension of finite residue fields; this in turn yields two key parameters.

4-22 PROPOSITION. *The finite extension k_1 of k satisfies the inequality $\text{mod}_{k_1}(p) < 1$ and therefore is likewise ultrametric. Moreover, $A_1 \cap k = A$ and $P_1 \cap k = P$.*

PROOF. In light of the topological and algebraic characterizations of A, P, A_1, and P_1, only the first statement requires justification. This follows from the general formula

$$\text{mod}_{k_1}(a) = \text{mod}_k(a)^n \quad (a \in k)$$

applied to $p \cdot 1_k$ to show that $\text{mod}_{k_1}(p)$ is also less than 1. ❑

We come now to a fundamental relationship between the degree of the extension k_1/k and the order of π, the uniformizing parameter in A, as an element of A_1.

4-23 PROPOSITION. *Let k_1/k be an extension of fields of degree n as above and define q_1, q, and e as follows:*

$$\begin{aligned} q_1 &= \text{Card}(A_1/P_1) \\ q &= \text{Card}(A/P) \\ e &= \text{ord}_{k_1}(\pi) \end{aligned}$$

Then $q_1 = q^f$ for some integer f, and moreover, $n = ef$ for some positive integer e.

PROOF. Certainly A_1/P_1 is a finite extension of the finite field A/P, whence such an exponent f exists. Using Eq. 4.4, we can compute $\text{mod}_{k_1}(p)$ in two ways:

$$\text{mod}_{k_1}(\pi) = (q_1)^{-e} = q^{-ef}$$

$$\text{mod}_{k_1}(\pi) = \text{mod}_k(\pi)^n = q^{-n}$$

A comparison of exponents yields the stated result. ❑

The integers e and f appearing in this proposition are singled out in the following definition.

DEFINITIONS. The invariant e is called the *ramification index* of k_1/k; the extension is called *unramified* if $e=1$. The exponent f is called the *residual degree* of k_1/k; the extension is called *totally ramified* if $f=1$.

Characterization of Unramified Extensions

We maintain the assumptions and notation of the previous subsection. In particular, k_1/k is an extension of nondiscrete locally compact fields and $\mathrm{mod}_k(p)<1$. Henceforth $\bar{k}$ and $\bar{k}_1$ denote, respectively, the residue fields associated with the local rings of k and k_1. Thus by definition $[\bar{k}_1:\bar{k}]=f$ and $q_1=q^f$. In accordance with our convention, M_1^* denotes the set of roots of unity in k_1 of order prime to p, and $M_1=M_1^*\cup\{0\}$.

4-24 LEMMA. *Let k_1 be a finite extension of k generated by one or more roots of unity of order prime to p. Then:*

(i) *$k_1=k(M_1)$; k_1 is thus the splitting field for the polynomial $x^{q_1-1}-1$ and hence a Galois extension of k.*

(ii) *Every automorphism $\sigma\in\mathrm{Gal}(k_1/k)$ induces an automorphism on the residue field $\bar{\sigma}\in\mathrm{Gal}(\bar{k}_1/\bar{k})$; moreover, the mapping $\sigma\mapsto\bar{\sigma}$ constitutes an isomorphism of groups.*

(iii) *k_1 is cyclic and unramified over k.*

PROOF. We know by the isomorphism $M_1^*\cong(A_1/P_1)^*$ (Proposition 4-19) that M_1^* consists precisely of the roots of $x^{q_1-1}-1$, and we have seen that k_1 at least contains M_1, whence by assumption $k_1=k(M_1)$. The subsets A_1 and P_1 both remain invariant under every (necessarily topological) automorphism σ of k_1 over k, so σ indeed induces the automorphism $\bar{\sigma}$ of $\bar{k}_1$ over $\bar{k}$ defined by $\sigma(a+P_1)=\sigma(a)+P_1$. If $\bar{\sigma}$ is the identity on $\bar{k}_1$, then $\sigma(a)\equiv a \pmod{P_1}$ for all $a\in k_1$. But since M_1 is a complete set of coset representatives for (A_1/P_1) and σ permutes the elements of M_1, this implies that $\sigma(a)=a$ for all $a\in M_1$. Hence σ is the identity on all of $k_1=k(M_1)$, and therefore the group homomorphism $\sigma\mapsto\bar{\sigma}$ is at least injective. From this we deduce at once that

$$ef=[k_1:k]\le[\bar{k}_1:\bar{k}]=f\ .$$

Thus the ramification index e must be 1—which is to say that k_1/k is unramified—and accordingly both Galois groups have the same cardinality. But if this is the case, then injectivity implies bijectivity for the map $\sigma \mapsto \bar{\sigma}$, whence $\mathrm{Gal}(k_1/k) \cong \mathrm{Gal}(\bar{k}_1/\bar{k})$, and the extension k_1/k is indeed cyclic by elementary Galois theory. This completes the proof. ❑

4-25 PROPOSITION. *Let k_1/k be a finite extension of nondiscrete locally compact fields with $\mathrm{mod}_k(p)<1$. Then k_1 is unramified over k if and only if k_1 is generated over k by M_1. Hence for every positive f, k has exactly one unramified extension of degree f, and this is generated over k by any primitive (q^f-1)th root of unity.*

PROOF. Assume that k_1/k is unramified of degree f and consider the intermediate extension $l=k(M_1)$, with residue field $\bar{l}$. Since M_1 also constitutes the set of roots of unity in $k(M_1)$ of order prime to p, it follows that M_1 is isomorphic to both $\bar{l}$ and $\bar{k}_1$; thus $[\bar{l}:\bar{k}] = [\bar{k}_1:\bar{k}] = f$. But then $[l:k]\geq f$, showing that $k_1=l$. In light of the previous lemma, this establishes the first statement and shows further that an unramified extension of degree f is precisely the splitting field over k of the polynomial $x^{q^f-1}-1$; it is therefore unique up to isomorphism. ❑

4-26 COROLLARY. *Let k_1/k be as above. Then the following assertions hold:*

(i) *The mapping $k_1 \mapsto \bar{k}_1$ constitutes a bijective correspondence between the isomorphism classes of unramified finite algebraic extensions of k and the isomorphism classes of finite extensions of $\bar{k}$.*

(ii) *Given any finite extension k_1 of k, there exists an unramified subextension l/k such that k_1/l is totally ramified.*

PROOF. Part (i) is immediate from the previous proposition, since a finite field is determined (up to isomorphism) by its order. For part (ii), take $l = k(M_1)$. Then l/k is maximally unramified and of degree f, the ramification index of k_1 over k. For a uniformizing parameter π of the local ring associated with k, the following equations hold:

$$\mathrm{ord}_{k_1}(\pi) = e$$
$$\mathrm{ord}_l(\pi) = 1$$

In particular, π is also a uniformizing parameter for the local ring associated with l, so that $e_{k_1/l} = e$. Since $[k_1:k] = ef$, it follows that $[k_1:l]=e$, $f_{k_1/l} = 1$, and k_1/l is totally ramified, as required. ❑

Finally, these results allow us to define the *Frobenius automorphism* associated with the unramified extension of any given degree. We shall study this in detail in Chapter 6.

DEFINITION. Let k_1/k be the unramified extension corresponding to the residue extension $\bar{k}_1/\bar{k}$ where $\bar{k} = \mathbf{F}_q$. Then φ_q is the automorphism of $\mathrm{Gal}(k_1/k)$ corresponding to the mapping $x \mapsto x^q$ in $\mathrm{Gal}(\bar{k}_1/\bar{k})$ under the isomorphism given above by Lemma 4-24, part (ii).

4.4 Places and Completions of Global Fields

A *number field* is a finite extension of $\mathbf{Q}$. A *function field in one variable* over a field k is a field extension K of k of transcendence degree 1. Hence K is an algebraic extension of the intermediate field $k(x)$ for some element $x \in K$ that is transcendental over k.

Since number fields are likely to be quite familiar, we will say a few words only about function fields. If X is any compact Riemann surface (i.e., a one-dimensional complex manifold), the field $K = \mathbf{C}(X)$ of meromorphic functions on X is a function field over the field of complex numbers (whence the name). In fact, every function field in one variable over $\mathbf{C}$ arises in this way. One also knows that every compact Riemann surface is the set of complex points of a smooth, projective algebraic curve over $\mathbf{C}$. Given a function field K in one variable over any field k, we may identify K with the field of rational functions of a smooth projective algebraic curve X over k. K is purely transcendental if and only if X has genus zero, which is to say that it is isomorphic to $\mathbf{P}_k^1$.

DEFINITION. A *global field* is one of the following:

(i) an algebraic number field K;

(ii) a finitely generated function field K in one variable over a finite field $k = \mathbf{F}_q$.

That these types of fields have many common properties has become the basis of one of the most fruitful analogies in mathematics.

Absolute Values

We study global fields mainly by analyzing the different types of "absolute values" they admit. Note that the function mod_k studied for local fields in the previous two sections is a particular instance of the following definition.

DEFINITION. Let F be a field. An *absolute value* (or *valuation of order* 1) on F is a map

$$|\cdot| : F \to \mathbf{R}_+$$

satisfying the following properties:

(AV-1) $|a|=0$ if and only if $a=0$.

(AV-2) $|ab|=|a|\cdot|b|$ for all $a,b\in F$.

(AV-3) There exists a positive real constant c such that for all $a,b\in F$ we have that $|a+b|\leq c\cdot\sup\{|a|,|b|\}$.

Note that the ordinary absolute value function on the complex numbers is an absolute value in the sense above with $c=2$. In fact, a somewhat stronger statement is true.

4-27 LEMMA. *Let* $|\cdot|: F\to\mathbf{R}_+$ *satisfy properties* AV-1 *and* AV-2. *Then the following statements are equivalent:*

(i) *Property* AV-3 *holds with* $c\leq 2$.

(ii) *For all* $a,b\in F$, $|a+b|\leq|a|+|b|$.

Statement (ii) is, as usual, called the *triangle inequality*.

PROOF. We need only show that (i) implies (ii). Assume that $n=2^m$ for some positive integer m and let $a_1,\ldots,a_n$ be a sequence of elements of F. Then by induction it follows at once that

$$|\sum_{j=1}^{2^m} a_j|\leq 2^m\cdot\sup|a_j|\ .$$

Now suppose that n is an arbitrary positive integer. We can always pad the sequence $a_1,\ldots,a_n$ with zeros out to 2^m terms, where m satisfies the condition $2^m\geq n>2^{m-1}$. The previous inequality then implies that

$$\begin{aligned}|\sum_{j=1}^{n} a_j| &\leq c\cdot\sup\{|\sum_{j=1}^{2^{m-1}} a_j|,\ |\sum_{j=2^{m-1}+1}^{2^m} a_j|\}\\ &\leq 2\cdot\sup\{\ 2^{m-1}\cdot\sup_{j\leq 2^{m-1}}|a_j|,\ 2^{m-1}\cdot\sup_{j>2^{m-1}}|a_j|\}\\ &\leq 2\cdot 2^{m-1}\cdot\sup_j|a_j|\ .\end{aligned}$$

Thus we achieve the general relation

$$|\sum_{j=1}^{n} a_j|\ \leq\ 2n\cdot\sup|a_j|$$

for arbitrary $n>0$. In particular, setting $a_j=1$ for all j, we obtain the inequality $|n|\le 2n$. Moreover,

$$|\sum_{j=1}^{n} a_j| \le 2n\cdot\sum_{j=1}^{n}|a_j| \quad .$$

We may now proceed with the main calculation:

$$\begin{aligned}
|a+b|^n &= |(a+b)^n| \\
&= |\sum_{j=0}^{n}\binom{n}{j}a^j b^{n-j}| \\
&\le 2(n+1)\sum_{j=0}^{n}|\binom{n}{j}||a|^j|b|^{n-j} \\
&\le 4(n+1)\sum_{j=0}^{n}\binom{n}{j}|a|^j|b|^{n-j} \\
&= 4(n+1)(|a|+|b|)^n \quad .
\end{aligned}$$

Taking the nth roots of both sides and then the limit as $n\to\infty$ now yields the triangle inequality. ❑

Note that if $|\cdot|$ is an absolute value, then $|1|=1$. Indeed, by AV-2, if $\alpha=|1|$, then $\alpha^2=\alpha$, whence α is 0 or 1. But the possibility that $\alpha=0$ is excluded by AV-1, whence $\alpha=1$.

One says that $|\cdot|$ is *trivial* if $|a|=1$ for all nonzero $a\in F$. Every absolute value on a finite field $k=\mathbf{F}_q$ is trivial. This is so because for any nonzero $a\in k$, we have $a^{q-1}=1$; accordingly $|a|^{q-1}=1$, and hence $|a|=1$, since $\mathbf{R}_+$ has no roots of unity other than 1.

DEFINITION. Two absolute values $|\cdot|$ and $|\cdot|'$ on F are *equivalent* if there is a positive constant t such that $|a|'=|a|^t$ for all $a\in F$. A *place* of F is an equivalence class of nontrivial absolute values.

Note that if we replace an absolute value $|\cdot|$ satisfying AV-3 for some $c>0$ by $|\cdot|^t$ for some $t>0$, then c is replaced by c^t. Appealing to the previous lemma, we see that every absolute value is equivalent to one that satisfies the triangle inequality.

The next proposition is similar in both form and proof to the corresponding statement for the function mod_k on a local field (Proposition 4-11).

4-28 PROPOSITION. *Let* $|\cdot|$ *be an absolute value on* F. *Then the following statements are equivalent:*

(i) $|\cdot|$ *satisfies the ultrametric inequality* (i.e., AV-3 with $c=1$).

(ii) *The set* $\{|n| : n\in\mathbf{N}\}$ *is bounded.*

In either case, $|n|$ *is in fact bounded by* 1 *on* $\mathbf{N}$.

PROOF. That the first statement implies the second follows at once from the observation that

$$|n| = |1+1+\cdots+1| \leq 1 \ .$$

Conversely, suppose that $|n|$ is bounded by some positive constant β for all natural numbers n. Then since $|\cdot|$ is multiplicative, $|n|$ cannot be greater than 1 for any n, or else $|n^m|$ tends to infinity. Replacing $|\cdot|$ by an equivalent absolute value if necessary, we may assume that $|\cdot|$ satisfies AV-3 with $c\leq 2$ and hence satisfies the triangle inequality. Thus we may calculate as in the previous result:

$$\begin{aligned} |a+b|^n &\leq \sum_{j=0}^{n} \left|\binom{n}{j}\right| |a|^j |b|^{n-j} \\ &\leq (n+1)\sup\{|a|,|b|\}^n \ . \end{aligned}$$

Taking the nth roots of both sides and then the limit as $n\to\infty$ now yields the ultrametric inequality. ❑

DEFINITION. An absolute value is called *non-Archimedean*, or *ultrametric*, if the equivalent conditions of the preceding proposition are satisfied. Otherwise it is called *Archimedean*, or *ordinary*.

Note that any absolute value $|\cdot|$ on a field F defines a nonnegative function d on $F\times F$ by

$$d(a,b) = |a-b| \ .$$

This function induces a topology on F, a base for which is given by open balls relative to d, and this topology is nondiscrete if and only if the absolute value is nontrivial. Clearly any equivalent absolute value induces the same topology (one can also establish the converse), and d may in fact be taken as a metric on F. We say that F is *complete* with respect to $|\cdot|$ if F is a complete metric space with respect to the metric topology defined by this absolute value. Thus, for example, every local field with its associated absolute value (the module) is

complete in this sense. The familiar construction of equivalence classes of Cauchy sequences yields the following result:

4-29 PROPOSITION. *Let F be an arbitrary field and let $|\cdot|$ be an absolute value on F. Then F can be embedded in a field that is complete with respect to an absolute value that is equivalent to $|\cdot|$ on F.*

Ostrowski's Theorem

We shall now classify the places of *prime global fields*; that is, either the rational numbers $\mathbf{Q}$ or a function field $\mathbf{F}_q(t)$.

4-30 THEOREM. *Let K be a prime global field. Then*

(i) *Suppose that $K=\mathbf{Q}$. Then every nontrivial place of K is represented by either the usual absolute value, sometimes denoted $|\cdot|_\infty$, or a p-adic one $|\cdot|_p$, for some prime p.*

(ii) *Suppose that $K=\mathbf{F}_q(t)$, and let $R=\mathbf{F}_q[t]$. Then every nontrivial place of K is given by either the "infinite place" $|\cdot|_\infty$ defined by*

$$|f/g|_\infty = q^{\deg(f)-\deg(g)}$$

or by the finite place $|\cdot|_P$ corresponding to an irreducible polynomial $P(t)\in R$.

The first statement is called Ostrowski's theorem.

PROOF. Note that in either case we must have $|z|=1$ for any root of unity z. Indeed, if $z^n=1$, then $|z|^n=1$, and so $|z|=1$, since there are no other roots of unity among the nonnegative reals. We now address the two separate cases.

(i) Suppose first that $|\cdot|$ is ultrametric; the analysis is similar to that for an ultrametric module. For any positive integer n, we know by induction that $|n|\leq 1$. Since $|\cdot|$ is nontrivial, $|n|<1$ for some positive integer, and we take n to be the smallest such. We claim that n must be prime. For if $m=m_1m_2$ where both factors are greater than 1, then the inequality $1>|m|=|m_1||m_2|$ implies that $|m_i|<1$ for at least one i, contradicting the minimality of m. Thus m is prime, and accordingly we shall henceforth write p for m.

We claim next that $|a|=1$ for any integer a prime to p. Indeed, any such a is of the form $dp+r$ for integers d and r with $0<r<p$. The choice of p forces $|r|$ to be 1. But since $|r|\leq\max\{|dp|,|a|\}$, this forces $|a|$ to be 1, as asserted. In summary, we have shown that

$$|ap^k| = |p|^k$$

for all k where a is prime to p. The usual p-adic norm has the same form with $|p|_p=1/p<1$, and it is now clear that $|\cdot|$ and $|\cdot|_p$ are equivalent.

Now consider the case that $|\cdot|$ is Archimedean and hence may be assumed to satisfy the triangle inequality. Then when restricted to **N**, this absolute value function satisfies the hypothesis of Proposition 4-10 with $A=2$. Since it is moreover unbounded, it follows from that same proposition that $|\cdot|$ is just a positive power of the ordinary absolute value function, and therefore it represents the same place of **Q**. This completes the proof of part (i).

(ii) We may identify the subring of K generated by $1\in K$ with the finite field $\mathbf{F}_p$. Thus the set of values $|n\cdot 1|$ for $n\in\mathbf{Z}$ is bounded, and hence $|\cdot|$ is non-Archimedean; in fact, these norms are precisely 1 for all n prime to p,.

Suppose that there exists a polynomial $P\in\mathbf{F}_q[t]$ such that $|P|<1$; clearly we may assume that P is irreducible. Then arguing as above, $|Q|=1$ for all Q not divisible by P. Hence given any polynomial $f\in\mathbf{F}_q[t]$, we may factor it into the form P^nQ where $n\geq 0$ and Q is prime to P, and thus $|f|=|P|^n$ in accordance with the second alternative of the assertion.

Now suppose that $|P|\geq 1$ for every irreducible polynomial $P\in\mathbf{F}_q[t]$. Then since $|a|=1$ for all nonzero constants, it follows that $|\cdot|$ maps $\mathbf{F}_q[t]^*$ into the interval $[1,\infty)$. Thus in particular, $|t|\geq 1$, and we claim that in fact this inequality is strict. Suppose to the contrary that $|t|=1$. We will then show that $|\cdot|$ takes the value 1 on all of K^*, contradicting the assumption that $|\cdot|$ represents a nontrivial place. For this it clearly suffices to show that $|f|=1$ for all $f\in\mathbf{F}_q[t]^*$, and accordingly we can proceed by induction on n, the degree of f. The case $n=0$ is clear. So assume that n is positive and write

$$f(t) = a_0 + t\varphi(t)$$

where $\varphi\in\mathbf{F}_q[t]^*$ is of degree $n-1$. By assumption and induction, $|t\varphi(t)|=1$, whence $|f|=1$, as claimed, because $|\cdot|$ is non-Archimedean. So indeed $|t|>1$.

We claim next that for a nonzero polynomial f we have $|f|=|t|^{\deg(f)}$. Again the proof goes by induction on n, the degree of f, and again the case that $n=0$ is clear. Writing f as above, we find at once that

$$|f(t)|\leq|t\varphi(t)|=|t|^n \ .$$

But then $|f|$ must be $|t|^n$, for otherwise we have a contradiction from the inequality

$$|t\varphi(t)|\leq \sup\{|a_0|,|f(t)|\}$$

since $|a_0|$ is 0 or 1. (We observe yet again that all non-Archimedean triangles are isosceles!) This proves the claim and also the theorem, because clearly

$$\left|\frac{f}{g}\right| = \frac{|f|}{|g|} = |t|^{\deg(f)-\deg(g)} . \qquad \square$$

Extension of Absolute Values

Let K denote an arbitrary global field. Let F denote a subfield of K of the form $\mathbf{F}_q(t)$ if K is of positive characteristic p or let $F=\mathbf{Q}$ if K has characteristic zero. In the former case, we can always find an element $t\in K$ such that K is finite and separable over $\mathbf{F}_q(t)$ (see Exercise 4), and hence we may assume that K/F is finite and separable.

Next put $n=[K:F]$ and for any place v of K, let K_v denote the completion of K relative to a representative absolute value, say $|\cdot|_v$, belonging to the class v. Let $\mathscr{P}_K$ denote the set of all places of K. This is the disjoint union of two subsets:

$$\mathscr{P}_{K,\infty} = \text{ the set of Archimedean places of } K, \text{ and}$$

$$\mathscr{P}_{K,f} = \text{ the set of ultrametric places of } K.$$

Note that every $v\in\mathscr{P}_K$ induces by restriction a place $u=\mathrm{res}_F(v)\in\mathscr{P}_F$, and hence we have defined a restriction map

$$\begin{aligned} r = r_{K/F}: \mathscr{P}_K &\to \mathscr{P}_F \\ v &\mapsto u \end{aligned}$$

from the places of K to the places of F.

Since the previous discussion gives a complete description of $\mathscr{P}_F$, to understand $\mathscr{P}_K$, it suffices to describe the image and the fibers of r.

Henceforth we shall write $v|u$ if $v\in r^{-1}(u)$ and say that v *lies over* u or that v *divides* u.

To analyze the relationship between local extensions K_v/F_u and the global extension K/F, we must analyze the embeddings over F of K into $\overline{F}_u$, the algebraic closure of the completion of F at u. By separability we know that $K=F(\alpha)$ for some element $\alpha\in\overline{F}\subseteq\overline{F}_u$. Let $p(x)$ denote the minimal polynomial of α over F and suppose that

$$p(x) = \prod_{j=1}^{r} p_j(x)$$

is the irreducible factorization of $p(x)$ in $F_u[x]$. For each j, fix a root α_j of $p_j(x)$ in $\overline{F}_u$. Note that these α_j are distinct, since $p(x)$ is separable.

4-31 PROPOSITION. *Let $K=F(\alpha)$ be a finite separable extension of F, where F is either $\mathbf{Q}$ or $\mathbf{F}_q(t)$, and let u be a fixed place of F. Suppose further that $p(x)$ is the minimal polynomial of α over F and that $p(x)$ factors over F_u into the product of polynomials $p_j(x)$ with corresponding roots α_j, as above ($j=1,\dots,r$). Then the following assertions hold:*

(i) *If v is a place of K that lies over u, then $K_v=F_u(\beta)$, where β is a root of $p(x)$ and hence separable over F_u. In particular, K_v/F_u is a finite separable extension.*

(ii) *The places v of K that lie over u are in bijective correspondence with the embeddings of K into $\overline{F}_u$ induced by the assignments $\alpha \mapsto \alpha_j$.*

PROOF. (i) Consider this diagram of embeddings:

$$\begin{array}{ccc} \overline{F} & & \overline{K}_v \\ | & & | \\ K=F(\alpha) & \to & K_v \\ | & & | \\ F & \to & F_u \end{array}$$

Clearly K_v contains $F_u(\beta)$, where β is the image of α and therefore a root of $p(x)$. But $F_u(\beta)$ is finite-dimensional over F_u and hence locally compact. Thus it is a complete field containing both F and the image of α, which is to say that $K_v=F_u(\beta)$.

(ii) Every finite extension $F_u(\beta)$ admits a unique topological structure as a locally compact field, namely the one induced by a vector space isomorphism with $(F_u)^m$, where m is the degree of β over F_u, and the associated absolute value on F_u. In particular, each of the extensions $F_u(\alpha_j)$ admits an absolute value, which, when restricted to the image of K, induces an absolute value on K and a corresponding place v that obviously lies over u. Part (i) shows that every such place arises in this way, since $F_u(\beta)$ is isomorphic to $F_u(\alpha_j)$ for some j.

It remains to show that distinct assignments $\alpha \mapsto \alpha_j$ give rise to distinct places. Consider, for instance, $p_1(x) \in F_u[x]$, which can be expressed—in the obvious sense—as the limit of a sequence $\{q(x)\}$ of polynomials over F. Then

$$|\lim q(\alpha)|_1 = |\lim q(\alpha_1)|_1 = |p_1(\alpha_1)|_1 = 0$$

where $|\cdot|_j$ denotes the absolute value associated with the embedding $\alpha \mapsto \alpha_j$. But for $j>1$,

$$|\lim q(\alpha)|_j = |\lim q(\alpha_j)|_j = |p_1(\alpha_j)|_j \neq 0$$

which shows that $|\cdot|_1$ and $|\cdot|_j$ represent different places. More generally then, $|\cdot|_j$ and $|\cdot|_k$ represent different places whenever $j \neq k$, as required. This completes the proof. ❑

As an immediate consequence of this proposition, we have the following fundamental result.

4-32 COROLLARY. *Let F, K, and u be as above and let $n=[K:F]$.*

(i) *Define $n_v=[K_v:F_u]$ for $v|u$. Then*

$$n = \sum_{v|u} n_v \ .$$

In particular, the restriction map is surjective, and the fiber over each place of F_u is finite.

(ii) *If K/F is moreover a Galois extension, then n_v is constant for all $v|u$.*

PROOF. (i) The proof of the first statement is immediate because the degree of K/F is also the degree of $p(x)$, while the degree of each local extension K_j/F_u is the degree of the corresponding factor $p_j(x)$.

(ii) If K/F is Galois, all of the roots of $p(x)\in F[x]$ lie in K, whence every embedding of K into $\overline{F}_u$ contains all of the roots of $p(x)$. Thus for all indices j and k, $F_u(\alpha_j)\subseteq F_u(\alpha_k)$, so that all of the completions of K in fact give rise to the same subfield of $\overline{F}_u$—only the embeddings are different—and hence are of the same dimension. ❑

We next analyze $n_v=[K_v:F_u]$ where $v|u$ in the case that u is ultrametric. Then K_v/F_u is a finite extension of non-Archimedean local fields. Let

$$\mathfrak{o}_u = \{x\in F_u : |x|_u \leq 1\} \quad \text{and} \quad \mathfrak{o}_v = \{x\in K_v : |x|_v \leq 1\}$$

denote the respective local rings of integers of K_v and F_u, and let k and k' denote the residue fields of $\mathfrak{o}_u$ and $\mathfrak{o}_v$ modulo their respective maximal ideals. Put

$$f_v = [k':k] \ .$$

This is called the *residual degree* of K_v over F_u.

4-33 LEMMA. *For all $v|u$, we have*

$$n_v = e_v f_v$$

for some integer e_v.

In this context, the positive integer e_v is called the *ramification index* of K_v over F_u. Note that our current use of the terms *residual degree* and *ramification index* is consistent with that of Section 4.2.

PROOF. Let L/F_u be the largest unramified subextension of K_v/F_u. Then, as we noted earlier in our characterization of unramified extensions (see especially Lemma 4-24 and Proposition 4-25), the residue field of L identifies with k', and moreover, $[L:F_u]=[k':k]=f_v$. Put $e_v=[K_v:L]$. The lemma follows. ❑

4-34 COROLLARY. *Let K/F be a finite separable extension of global fields, and let u be a non-Archimedean place of F. Then we have*

$$n=[K:F]=\sum_{v|u} e_v f_v \quad .$$

Moreover, if K/F is Galois, then both the ramification indices and the residual degrees are constant for all v lying over u, so that

$$n = efg$$

where $e=e_v$, $f=f_v$, and g is the number of places v of K lying over u.

PROOF. Since for a Galois extension we already know that $n_v=e_v f_v$ is constant, it suffices to show that the residual degree is invariant. But in this case, all of the local extensions are isomorphic to a single finite extension, say, K_v of F_u. The maximal unramified subextension of K_v is obtained from F_u by adjoining all of the roots of unity of order prime to the characteristic and hence is also independent of v. Finally, f_v is precisely the degree of this subextension. ❑

DEFINITION. The finite extension K/F is *unramified at u* if $e_v=1$ for all $v|u$. It is *totally ramified* if $f_v=1$ for all $v|u$.

DEFINITION. *Let E* be an algebraic extension of a number field F, possibly of infinite degree. Then we say that E/F is *unramified* (respectively, *totally ramified*) at a place u of F if there exists a chain

$$F=E_0\subseteq E_1\subseteq\cdots\subseteq E=\bigcup E_i$$

of finite extensions such that each E_i/E_{i-1} is unramified (respectively, totally ramified) at every place of E_{i-1} lying above u.

The Ring of Integers of a Global Field

Let K be a global field. If K is a number field, then the ultrametric places of K are also called *finite places*; the Archimedean ones are also called *infinite places.*

If $p=\text{char}(K)$ is positive, we fix an element $t \in K$ such that K is a finite separable extension of $\mathbf{F}_q(t)$ with $\mathbf{F}_q = K \cap \mathbf{F}_p$. Here t is not canonically defined, but this is of no consequence to what follows. We shall now define the *infinite places* of K to be those lying over that place of $\mathbf{F}_q(t)$ represented by

$$|f/g|_\infty = q^{\deg(f)-\deg(g)} \ .$$

The remaining places of K are then called *finite*. We emphasize that in the function field case, the distinction between finite and infinite places does not correspond to the dichotomy of the ultrametric versus the Archimedean.

DEFINITION. Let K be a global field, with finite and infinite places defined as above. Then we define $\mathfrak{o}_K$, the *integers* of K, as follows:

$$\mathfrak{o}_K = \bigcap_{v \text{ finite}} \{x \in K : |x|_v \leq 1\} \ .$$

Thus $\mathfrak{o}_K$ is the intersection of the local rings of integers at all finite places of K and is therefore itself a ring.

In consonance with this definition we shall in the sequel often write $\mathfrak{o}_{K_v}$ for what we had previously denoted $\mathfrak{o}_v$ when we wish to emphasize the underlying local field.

The proposition below summarizes the most important properties of the integers of a global field. The proof is largely elementary algebra and is therefore omitted.

4-35 PROPOSITION. *The ring of integers $\mathfrak{o}_K$ of a global field K has the following properties:*

(i) *$\mathfrak{o}_K$ is a Noetherian domain that is integrally closed in its field of fractions; moreover, every prime ideal of $\mathfrak{o}_K$ is maximal.*

(ii) *$\mathfrak{o}_K$ is in fact the integral closure of $\mathbf{Z}$ in K if K has zero characteristic, and the integral closure of $\mathbf{F}_q[t]$ in K if K has positive characteristic.* ❑

Part (i) says that $\mathfrak{o}_K$ is a *Dedekind domain*, from which it follows that every nonzero element or ideal is contained in only finitely many prime ideals. (See Appendix B.) This tells us in particular that the fraction field of $\mathfrak{o}_K$ is in fact K itself.

Henceforth, for K a global field, a *prime of* K is simply a nonzero prime ideal of the ring of integers $\mathfrak{o}_K$. One shows easily that the quotient field $\mathfrak{o}_K/Q$ (computed globally) is isomorphic to the local version $\mathfrak{o}_v/Q_v$, where v is the ultrametric place associated with the prime Q. In particular, this quotient is finite. We shall often write K_Q rather than K_v to denote the completion of K at the place corresponding to Q; similarly we often write $\mathfrak{o}_Q$ for $\mathfrak{o}_v$.

If K/F is an extension of global fields, then we say that a prime Q of K *lies above* a prime P of F if either of the following equivalent conditions holds: (i) the place of K corresponding to Q lies above the place of F corresponding to P, or (ii) $P \subseteq Q$.

4.5 Ramification and Bases

We close this chapter with two principal results. The first places a finite limit on the number of primes that ramify in a finite separable extension K/F of global fields. The second, which is quite technical, describes how we pass from a global basis of K/F to a basis of the product of local extensions K_v/F_u relative to a fixed place u of F. This is essential to our geometric analysis of the adele group in the following chapter.

Ramification and the Decomposition Group

Consider a finite Galois extension K/F of global fields with $G = \mathrm{Gal}(K/F)$, and let Q be a prime of K. Then Q lies above some prime P of F, and we let $\mathbf{F}$ denote the residue field $\mathfrak{o}_F/P$. We define the *decomposition group* of Q in G to be

$$D_Q = \{\sigma \in G \mid \sigma(Q) = Q\} \ .$$

Now suppose that the residue field $\mathfrak{o}_K/Q$ is the finite field $\mathbf{F}_q$, a finite extension of $\mathbf{F}$. We have a canonical homomorphism

$$\rho_Q : D_Q \to \mathrm{Gal}(\mathbf{F}_q/\mathbf{F})$$

that associates with $\sigma \in D_Q$ the map ($x \bmod Q \mapsto \sigma(x) \bmod Q$) for all $x \in \mathfrak{o}_K$. This makes sense because $\sigma(Q) = Q$ for all σ in the decomposition group of Q. Also, $\rho_Q(\sigma)$ is trivial on $\mathbf{F} = \mathfrak{o}_F/P$, since σ is trivial on F.

We shall have more to say later about the decomposition group in connection with the Frobenius elements, which we study in Chapter 6. For the moment we need only these elementary facts about the homomorphism ρ_Q:

4-36 PROPOSITION. *The canonical map* $\rho_Q : D_Q \to \mathrm{Gal}(\mathbf{F}_q/\mathbf{F})$ *has the following three properties:*

(i) ρ_Q *is surjective.*

(ii) ρ_Q *is also injective if and only if P is unramified in K; i.e., if and only if the local extension K_Q/F_P is unramified.*

(iii) *Each $\sigma \in D_Q$ extends to an automorphism of the completion K_Q that is trivial on the subfield F_P. The induced map*

$$j_Q : D_Q \to \mathrm{Gal}(K_Q/F_P)$$

is in fact an isomorphism.

PROOF. We first show that the order of D_Q is the degree of the local extension K_Q/F_P. Let $G=\mathrm{Gal}(K/F)$. Then G has order efg, where e and f are the common ramification index and residual degree of the primes lying over P, and g is the number of such primes. But since G acts transitively on the set of primes of K lying above P (see Exercise 5 below) and $\tau D_Q=\tau' D_Q$ if and only if $\tau(Q)=\tau'(Q)$, the integer g is also the index of D_Q in G. Hence $o(G)=g\cdot o(D_Q)$, whence the decomposition group of Q has order ef, the degree of the corresponding local extension. This proves the asserted equality.

We can now prove assertion (iii). Each $\sigma \in D_Q$ is by construction an isometry of K, and so the extension $j_Q(\sigma)$ clearly exists and respects F_P. Moreover, j_Q is injective: $j_Q(\sigma)$ cannot be trivial unless σ is. But as we have just shown, D_Q and $\mathrm{Gal}(K_Q/F_P)$ have common order, whence j_Q is indeed an isomorphism.

Next consider the commutative diagram

$$\begin{array}{ccc} D_Q & \xrightarrow{\quad \rho_Q \quad} & \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}) \\ & {\scriptstyle j_Q}\searrow \quad \nearrow{\scriptstyle \tilde{\rho}_Q} & \\ & \mathrm{Gal}(K_Q/F_P) & \end{array}$$

where $\tilde{\rho}_Q$ is the map $\sigma \mapsto (x \bmod Q \mapsto \sigma(x) \bmod Q)$. Let L/F_P denote the maximal subextension of K_Q/F_P such that L is unramified over F_P. From our analysis of unramified extensions in Section 4.3, we know that L/F_P is normal over F_p and that $\mathrm{Gal}(L/F_P)$ is isomorphic to $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F})$ by the "restriction" of $\tilde{\rho}_Q$ to $\mathrm{Gal}(L/F_P)$. This yields assertion (i), because ordinary restriction from K_Q to L yields a surjective homomorphism from $\mathrm{Gal}(K_Q/F_P)$ to $\mathrm{Gal}(L/F_P)$.

Finally, we deduce assertion (ii) from the triangle. Since $\mathrm{Gal}(L/F_P)$ already maps surjectively onto $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F})$, $\tilde{\rho}_Q$—and hence ρ_Q—is moreover injective exactly when $L=K_Q$; that is, exactly when the local extension is unramified. ❑

Our goal for the remainder of this subsection is to establish the following fundamental result, which will be critical to our subsequent discussion of local and global bases.

4-37 PROPOSITION. *Let K/F be a finite separable extension of global fields. Then there are at most finitely many primes P in F that ramify in K.*

REMARK. This is a far less precise statement than one might make using the notion of the relative discriminant of K/F, but the present assertion suffices for our purposes. (See Exercises 13, 14, and 15 below and Appendix B, Section 2.) Moreover, the nonstandard proof that we give uses a key idea found in the proofs of the Tchebotarev density theorem and the Artin reciprocity law, both stated in Chapter 6: the reduction to cyclotomic and Kummer extensions.

PROOF. The argument proceeds in four steps. The first three are reductive; the fourth is a direct argument for a much simplified special case.

STEP 1. *We may assume that K/F is finite and Galois.* Indeed, if K is not normal over F, let E be its normal closure. Then a prime P that ramifies in K must certainly ramify in E: the ramification index measures the order of the corresponding uniformizing parameter in a local extension K_Q/F_P, and this can only get larger if we pass to E. Thus it suffices to show that only finitely many primes ramify in E.

STEP 2. *We may assume that K/F is cyclic of prime degree, say l.* This is considerably more subtle. We claim that any given prime P of F ramifies in K if and only if there exists some intermediate field K_1, $K \supseteq K_1 \supseteq F$, such that

(i) K/K_1 is cyclic of prime degree, and

(ii) there exists a prime divisor P_1 of P in K_1 such that P_1 ramifies in K.

Certainly the backward direction is trivial, so suppose that P ramifies in K. Then there exists a prime divisor Q of P in K such that K_Q/F_P is ramified, with corresponding residue fields $\mathbf{F}_q$ and $\mathbf{F}$. But then the natural map

$$\tilde{\rho}_Q\colon \mathrm{Gal}(K_Q/F_P) \to \mathrm{Gal}(\mathbf{F}_q/\mathbf{F})$$

is surjective but not injective by the previous proposition. Let N denote the kernel of this map. Again by the previous proposition, we may identify N with a subgroup of the decomposition group D_Q, and of course K_Q is ramified over any intermediate field containing K_Q^N. Since $K_Q \neq K_Q^N$, we may choose an intermediate field L with $K_Q \supseteq L \supseteq K_Q^N$ and K_Q/L cyclic of prime degree. Let H be the subgroup of D_Q corresponding to $\mathrm{Gal}(K_Q/L)$ and put $K_1 = K^H$. Then K/K_1 is also

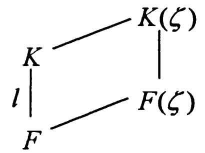
cyclic of prime degree. Let $P_1 = Q \cap \mathfrak{o}_{K_1}$, so that P_1 is a prime between P and Q, and the completion of K_1 at P_1 may be taken in K_Q. Now $\mathrm{Gal}(K/K_1)$ is contained in D_Q, so in fact the decomposition group of Q computed relative to K_1 is the full Galois group. Thus by the definition of K_1 and part (iii) of the previous proposition,

$$\mathrm{Gal}(K_Q/(K_1)_{P_1}) = \mathrm{Gal}(K/K_1) = \mathrm{Gal}(K_Q/L)$$

and therefore $(K_1)_{P_1} = L$. Since $K_Q/(K_1)_{P_1}$ is ramified by construction—after all, $\mathrm{Gal}(K/K_1)$ is also contained in N—we have established our assertion.

According to this claim, then, any prime that ramifies in K/F gives rise to a prime that ramifies in a cyclic intermediate extension of prime degree. But since there are only finitely many such intermediate extensions—indeed, intermediate extensions of *any* kind—it suffices to show that only finitely many primes ramify under these special conditions.

STEP 3. *We may assume that K/F is cyclic of prime degree l and that F contains all of the lth roots of unity in the algebraic closure of F.* If $l = p$, the characteristic of F, then the only lth root of unity is 1 itself, and the present case reduces trivially to that of the previous step. Hence we may assume for the balance of this step that l is different from p. Let ζ denote a nontrivial, hence primitive, lth root of unity in $\overline{F}$, and consider the following diagram of fields:



To verify our reduction, it suffices to show that there are only finitely many primes P in F that ramify in $F(\zeta)$. For then if there are only a finite number of primes of $F(\zeta)$ that ramify in $K(\zeta)$, there can only be finitely many primes of F that ramify in K.

Now consider the extension $F(\zeta)/F$. In the function field case, all of the residue fields have characteristic p, which is here assumed distinct from l. In the number field case, for only finitely many primes P of F is the corresponding residual field of characteristic l, since as we have seen, the restriction map for absolute values has finite fibers. In either case, for all but the finitely many primes whose residual characteristic is l, the local extension $F_P(\zeta)/F_P$ is unramified by Proposition 4-25. This concludes Step 3.

STEP 4. We shall now prove the proposition in the case that K/F is a cyclic Galois extension of prime degree l, with the further assumption that F contains all of the lth roots of unity in its algebraic closure.

If l is different from p, the characteristic of F, by standard Kummer theory we have $K=F(\alpha)$, with α a root of $f(x)=x^l-a$, for some $a \in F^*$, where a itself is not an lth power in F. If l is identical to p, then again $K=F(\alpha)$, but this time α is a root of $f(x)=x^p-x-a$, for some a as characterized previously. Let S be the set of primes P in F such that $|a|_P \neq 1$. Then S is finite, since $\mathfrak{o}_F$ is a Dedekind domain. Further define S' (again finite) by

$$S' = \begin{cases} S & \text{if } \operatorname{char}(F) > 0 \\ S \cup \{\text{primes } P \text{ with residual characteristic} \neq l\} & \text{if } \operatorname{char}(F) = 0\,. \end{cases}$$

The proof will be complete once we establish the following result:

4-38 LEMMA. *Suppose that P does not lie in S'. Then for any prime Q of K lying over P the local extension K_Q/F_P is unramified.*

PROOF OF LEMMA. Clearly the local extension is either trivial or cyclic of degree l. We may thus assume the latter case, so that α is a root of $f(x)$ in K_Q-F_P. Let L be the maximal unramified subextension of K_Q/F_P. We have the following diagram of local and residual fields:

$$\begin{array}{ccc} K_Q & \text{---} & \mathbf{F}_q \\ | & & | \\ L & \text{---} & \mathbf{F}_q \\ | & & | \\ F_P & \text{---} & \mathbf{F} \end{array}$$

Now we consider the consequences of the relation $f(\alpha)=0$. First note that whichever of the two forms that f takes, since a is a unit in $\mathfrak{o}_P$ (for P not in S, $|a|_P=1$!), it follows that α is itself a unit in $\mathfrak{o}_Q$ and, in particular, integral with respect to Q. Second, $f(x)$ has a root β in the residual field $\mathbf{F}_q$ that arises from an integer of the corresponding local field. This second statement clearly holds also at the middle level of the diagram above, and this is the key to the argument. Let us compute the formal derivative of $f(x)$:

$$f'(x) = \begin{cases} lx^{l-1} & \text{if } l \neq p \\ -1 & \text{if } l = p\,. \end{cases}$$

In either case $f'(\beta)$ is *not* congruent to zero modulo P, and Hensel's lemma (Exercise 6) applies—to the middle level!—to lift β to an integer of L. But then L contains a root of F and $K_Q=L$. Thus P is unramified. ❑

This complete the proof of the full proposition. ❑

REMARK. Note that the hypotheses of Hensel's lemma, namely that

(i) $f(\beta) \equiv 0 \pmod{P}$ and

(ii) $f'(\beta) \not\equiv 0 \pmod{P}$,

imply that f and f' do not have any roots in common; that is, the discriminant of f [or the resultant of (f,f')] is nonzero modulo P. This naturally leads to the use of the discriminant of K/F to determine which primes ramify—typically the more common approach.

Global and Local Bases

In this subsection, K/F is a finite separable extension of global fields. Let u be a place of F, and define M by

$$M = \prod_{v|u} K_v \ .$$

That is, M is the product of all the completions of K at places lying over u. We have an embedding

$$\begin{aligned} K &\overset{\psi}{\to} M \\ x &\mapsto \sum \psi_v(x) \end{aligned}$$

where ψ_v is the canonical embedding given by the completion at v. The following result is fundamental.

4-39 PROPOSITION. *Let $\{e_1,\ldots,e_n\}$ be an F-basis of K, and let u be a place of F. Then $X=\{\psi(e_1),\ldots,\psi(e_n)\}$ is an F_u-basis of M. Moreover, there exists a finite set S of places of F, containing the Archimedean ones, such that for all $u \notin S$,*

$$\mathfrak{o}_M = \prod_{v|u} \mathfrak{o}_{K_v}$$

is free over $\mathfrak{o}_{F_u}$ with basis X.

If L and M are extensions of a common field k, then $\mathrm{Hom}_k(L, M)$ denotes the set of embeddings of L into M that induce the identity map on k.

PROOF. Extend ψ to an F_u-linear map

$$\varphi : K \otimes_F F_u \to M$$

in the obvious way. Both sides are F_u-vector spaces of dimension n, since as we have just seen, the sum of the local degrees $[K_v : F_u]$ is precisely the dimension of K over F, and clearly $\{e_i \otimes 1\}_{1 \le i \le n}$ is an F_u-basis for the domain. Hence it suffices to show that φ is injective, in fact over $\overline{F}_u$. This requires one technical preliminary.

Recall from our discussion of local and global degrees that $K = F(\alpha)$ for some α and that every embedding of K into $\overline{F}_u$ over F is induced by an assignment $\alpha \mapsto \beta$, where β is a root of the minimal polynomial $p(x)$ of α over F. Moreover, the associated place induced on K depends exactly on the conjugacy class of β: the assignments $\alpha \mapsto \beta$ and $\alpha \mapsto \beta'$ give rise to the same place of K if and only if β and β' are roots of the same irreducible component of $p(x)$ when factored over F_u. The upshot of this discussion is that we can construct a bijection λ between the global and local embeddings into the algebraic closure of F_u as follows:

$$\lambda : \mathrm{Hom}_F(K, \overline{F}_u) \to \bigsqcup_{v|u} \mathrm{Hom}_{F_u}(K_v, \overline{F}_u)$$

$$\overset{\sigma}{(\alpha \mapsto \beta)} \mapsto \overset{\sigma_v}{(\psi_v(\alpha) \mapsto \beta)} \ .$$

We now proceed with the main body of the proof. Consider the following diagram:

$$\begin{array}{ccccc}
K \otimes_F \overline{F}_u & \xrightarrow{\varphi \otimes 1} & M \otimes_{F_u} \overline{F}_u & & \\
\kappa \downarrow & & & \searrow \Pi \kappa_v & \\
\overline{F}_u^{\,\mathrm{Hom}_F(K, \overline{F}_u)} & \underset{\lambda_*}{\longrightarrow} & \overline{F}_u^{\,\bigsqcup_{v|u} \mathrm{Hom}_{F_u}(K_v, \overline{F}_u)} & = & \prod_{v|u} \overline{F}_u^{\,\mathrm{Hom}_{F_u}(K_v, \overline{F}_u)}
\end{array}$$

where λ_* is the isomorphism induced from λ and κ is the $\overline{F}_u$-linear injection induced by the $\overline{F}_u$-bilinear map

$$K \times \overline{F}_u \to \overline{F}_u^{\mathrm{Hom}_F(K,\overline{F}_u)}$$
$$(x,y) \mapsto (\sigma(x)y)_{\sigma\in\mathrm{Hom}_F(K,\overline{F}_u)}$$

and similarly for each κ_v. Since by construction each embedding $\sigma: K \to \overline{F}_u$ factors as $K \xrightarrow{\psi_v} K_v \xrightarrow{\sigma_v} \overline{F}_u$ for some unique $v|u$, we have that

$$\lambda_*(\kappa(x\otimes y)) = \lambda_*((\sigma(x)y)_{\sigma\in\mathrm{Hom}_F(K,\overline{F}_u)}) = ((\sigma_v \circ \psi_v(x)y)_{\sigma_v\in\mathrm{Hom}_{F_u}(K_v,\overline{F}_u)})_{v|u}.$$

But also

$$\kappa_v((\varphi\otimes 1)(x\otimes y)) = \kappa_v((\psi_v(x))_{v|u}\otimes y) = (\sigma_v \circ \psi_v(x)y)_{\sigma_v\in\mathrm{Hom}_{F_u}(K_v,\overline{F}_u)}$$

and this is the same as the v-component of $\lambda_*(\kappa(x\otimes y))$. Hence the diagram is commutative, and it follows that $\varphi\otimes 1$ and φ are injections, as required.

We now prove the second assertion of the proposition. Let u be any finite place of F. Since $\mathfrak{o}_{F_u}$ is a discrete valuation ring and therefore a principal ideal domain, each $\mathfrak{o}_{K_v}$ is free over $\mathfrak{o}_{F_u}$, and thus $\mathfrak{o}_M$ is likewise free over $\mathfrak{o}_{F_u}$. The previous part shows that in fact the rank of $\mathfrak{o}_M$ is $\dim_{F_u}(M)=n$, the cardinality of the basis $X=\{\psi(e_1),\ldots,\psi(e_n)\}$. Let S' be the finite set of places consisting of the Archimedean ones, the unramified ones, and those corresponding to primes that divide the numerators or denominators of the e_j. Then X certainly lies in $\mathfrak{o}_M$ for all $u\notin S'$. Now consider the following claim:

CLAIM 1. *There exists a finite set $S\supseteq S'$ such that for all $u\notin S$, the collection $\{\psi(e_1),\ldots,\psi(e_n)\}$ spans* $\mathfrak{o}_M$ over $\mathfrak{o}_{F_u}$.

Granting this, the collection $\{\psi(e_1),\ldots,\psi(e_n)\}$ is clearly a basis for $\mathfrak{o}_M$ over $\mathfrak{o}_{F_u}$ for all $u\notin S$, as required.

To establish Claim 1, we consider the modules

$$L = \sum_j \mathfrak{o}_F e_j \text{ and } L_u = \sum_j \mathfrak{o}_{F_u}\psi(e_j) \cong L\otimes_{\mathfrak{o}_F}\mathfrak{o}_{F_u}.$$

Then $L_u\subseteq\mathfrak{o}_M\cong\mathfrak{o}_K\otimes_{\mathfrak{o}_F}\mathfrak{o}_{F_u}$ for all $u\notin S'$. (The isomorphism follows from the equality of dimensions.) The claim now follows, provided that $L_u=\mathfrak{o}_M$ for all but finitely many of these u. Let P_u be the unique prime ideal of $\mathfrak{o}_{F_u}$. Then by Nakayama's lemma it suffices to show that

$$L_u + P_u\,\mathfrak{o}_M = \mathfrak{o}_M$$

and since u is unramified, this amounts to establishing

$$L_u + (\prod_{v|u} P_v)\mathfrak{o}_M = \mathfrak{o}_M$$

where P_v is the unique prime ideal of $\mathfrak{o}_{K_v}$. This in turn follows almost everywhere from our next claim.

CLAIM 2. *For almost all places u, the elements* $\overline{\psi(e_j)}$ *span the product*

$$R = \prod_{v|u} \mathfrak{o}_{K_v}/P_v$$

over $\mathbf{F} = \mathfrak{o}_{F_u}/P_u$.

Here the bar denotes canonical projection into the quotient module. To prove this, put

$$I_u = \prod_{v|u} (P_v \cap K) \subseteq K \quad .$$

Then R identifies with $\mathfrak{o}_K/I_u$ by the Chinese remainder theorem, since the prime ideals $P_v \cap K$ are all also maximal; moreover, each $\psi(e_j)$ identifies with $\bar{e}_j$. Thus Claim 2 is equivalent to the following, which finally we prove directly:

CLAIM 3. *For almost all places u, we have*

$$(L + I_u)/I_u \supseteq \mathfrak{o}_K/I_u \quad .$$

PROOF OF CLAIM 3. Note that the indicated inclusion is equivalent to the statement that $\mathfrak{o}_K \subseteq L + I_u$. Put $\mathfrak{A} = L \cap \mathfrak{o}_K$. We have the following chain of equivalences:

$$\begin{aligned} \mathfrak{o}_K \not\subset L + I_u &\Leftrightarrow \mathfrak{o}_K \not\subset \mathfrak{A} + I_u \\ &\Leftrightarrow \mathfrak{A} + I_u \subseteq P_v \text{ for some } v|u \\ &\Leftrightarrow \mathfrak{A} \subseteq P_v \text{ for some } v|u \quad . \end{aligned}$$

The second equivalence follows because I_u is not contained in any maximal ideal other than P_v. But by the general theory of Dedekind domains, $\mathfrak{A}$ is contained in only a finite number of prime ideals of $\mathfrak{o}_K$, and hence we have the required inclusion for almost all u. ❑

Note that since $K\otimes_F F_u$ and $M=\prod_{v|u} K_v$ are both finite-dimensional of the same dimension, they acquire a canonical locally compact topological structure from F_u. Thus we end with the following useful result, whose proof is left as an exercise.

4-40 PROPOSITION. *The algebraic isomorphism $K\otimes_F F_u \to M=\prod_{v|u} K_v$ is in fact a topological isomorphism.* ❑

Exercises

1. Let α be an automorphism of a locally compact group G. Show that if G is discrete, then the module of α is 1.

2. Construct a strictly multiplicative $F:\mathbf{N}\to\mathbf{R}_+$ such that the conclusion of Proposition 4-10 does not hold. (In particular, F must not satisfy the given inequality.)

3. Let V be a locally compact topological vector space over a nondiscrete locally compact field k, and let W be a subspace of V. Show the following, *without* appeal to the fact that V must indeed be finite-dimensional over k (cf. Proposition 4-13):

(a) V is topologically isomorphic to $W\oplus W'$ for some subspace W' that is topologically isomorphic to V/W. Here W and W' have the topology induced by the projection maps $\mathrm{pr}_W(X)$ and $\mathrm{pr}_{W'}(X)$; i.e., the weakest topology that makes these projections continuous. (Note that both subspaces are trivially locally compact with respect to this topology.)

(b) If X is a Borel subset of V, then $\mathrm{pr}_W(X)$ and $\mathrm{pr}_{W'}(X)$ are Borel subsets of W and W', respectively.

(c) Let μ and μ' be Haar measures on W and W', respectively. Show that the product $\mu(\mathrm{pr}_W(X))\cdot\mu'(\mathrm{pr}_{W'}(X))$ is a Haar measure on V.

(d) Conclude that for each $a\in k$, $\mathrm{mod}_V(a)= \mathrm{mod}_W(a)\cdot\mathrm{mod}_{W'}(a)$.

4. Let K be a finitely generated extension of transcendence degree 1 of the finite field F. (Hence K is a global field.) Show that there exists an element u in K such that K is a finite separable extension of the function field $F(u)$.

5. Let K/F be a finite Galois extension of global fields, and let P be a prime of F. Show that $G=\mathrm{Gal}(K/F)$ acts transitively on the set of primes of K lying above P. [*Hint*: Let Q and Q' lie above P and suppose that $\sigma(Q)$ does not equal (and therefore is not contained in) Q' for all $\sigma\in G$. What, then, can

one say about $\prod_\sigma \sigma(Q)$? Does this product not lie in P? Must it not also then lie in the prime ideal Q'?]

6. (Hensel's Lemma) Let F be a non-Archimedean local field with ring of integers $\mathfrak{o}_F=\{\alpha\in F:|\alpha|\leq 1\}$ and prime ideal $P=\{x\in F:|x|<1\}$. Let $f\in\mathfrak{o}_F[x]$ be such that for some $a\in\mathfrak{o}_F$,

$$f(a)\equiv 0 \pmod P \quad \text{but} \quad f(a)\not\equiv 0 \pmod P \ .$$

Show that there exists $b\in\mathfrak{o}_F$ such that $f(b)=0$. Use this to show that F contains all of the qth roots of unity for $q=\mathrm{Card}(\mathfrak{o}_F/P)$.

7. (Krasner's Lemma) Let F be a non-Archimedean local field with algebraic closure $\overline{F}$. Suppose that $\alpha,\beta\in\overline{F}$ satisfy

$$|\beta-\alpha|<|\tau\alpha-\alpha| \quad \forall\tau\in\mathrm{Hom}_F(F(\alpha),\overline{F})$$

and that β is separable over $F(\alpha)$. Show that $F(\alpha)\subseteq F(\beta)$.

8. Let F be a non-Archimedean local field and let $f\in F[x]$ be a monic, irreducible, separable polynomial. Let g be another monic polynomial in $F[x]$ of the same degree. Identifying f and g as points in the metric space $F^{(\deg f+1)}$, show that if g is close enough to f, then g is also irreducible. Show also that there is a bijection $\{\alpha_i\}\leftrightarrow\{\beta_i\}$ between the roots of f and those of g such that $F(\alpha_i)=F(\beta_i)$ for all i. [*Hint*: Use the previous problem.]

9. Let F be a global field with non-Archimedean completion F_v, and let E/F_v be a finite extension of degree d. Show that there exists an extension K/F of degree d such that K embeds densely in E. [*Hint*: Use the previous exercises.]

10. Let F be a non-Archimedean local field. Show (i) that for every $n\geq 1$ there exists a unique unramified extension F_n of degree n. Now let F^{ur} denote the maximum unramified extension of F in its algebraic closure. Prove (ii) that we have the following isomorphism of topological groups:

$$\mathrm{Gal}(F^{\mathrm{ur}}/F)\cong\hat{\mathbf{Z}}=\varprojlim_n(\mathbf{Z}/n\mathbf{Z}) \ .$$

(See also Section 1.3.)

11. Let F be a non-Archimedean local field with prime ideal P and let E/F be a totally ramified extension of degree e. Show that any uniformizing element π of E satisfies an Eisenstein equation over F; i.e., an equation of the form

$$\sum_{j=0}^{e} a_j x^j = 0 \quad (a_j \in \mathfrak{o}_F, \forall j;\ a_e = 1; a_j \equiv 0 \bmod P, \forall j \le e-1;\ a_0 \not\equiv 0 \bmod P^2)\ .$$

12. Show that for all $n \ge 1$, a non-Archimedean local field has only a finite number of extensions of degree less than or equal to n. [*Hint*: Use the previous three exercises.]

13. Let K/F be a finite separable extension of non-Archimedean local fields, with respective rings of integers $\mathfrak{o}_K$ and $\mathfrak{o}_F$, and uniformizing parameters π_K and π_F. We define the *inverse different* (or *codifferent*) $\mathfrak{D}_{K/F}^{-1}$ of K over F to be $\pi_K^{-d}\mathfrak{o}_K$, where d is the largest integer such that $\mathrm{tr}_{K/F}(\pi_K^{-d}\mathfrak{o}_K) \subseteq \mathfrak{o}_F$. The *different* $\mathfrak{D}_{K/F}$ is then given by

$$\mathfrak{D}_{K/F} = \pi_K^d \mathfrak{o}_K$$

and the *discriminant* $\Delta_{K/F}$ by

$$\Delta_{K/F} = N_{K/F}(\pi_K^d)\mathfrak{o}_F$$

where $N_{K/F}$ is the norm map. Thus $\Delta_{K/F}$ is an ideal of $\mathfrak{o}_F$. (See Appendix B.2 for a more general treatment in the case of a Dedekind domain.)

REMARK. When F is either $\mathbf{Q}_p$ or $\mathbf{F}_q((t))$, one drops the expression "over F" and simply writes $\mathfrak{D}_K$ and Δ_K for the different and the discriminant, respectively.

(a) Let $n = [K:F]$. We know from the elementary theory of principal ideal domains that there exist elements $e_1, \ldots, e_n \in \mathfrak{o}_K$ that constitute a basis for $\mathfrak{o}_K$ over $\mathfrak{o}_F$. Use this fact to obtain the formula

$$\Delta_{K/F} = \Delta_{K/F}(e_1, \ldots, e_n)\ \mathfrak{o}_F$$

where

$$\Delta_{K/F}(e_1, \ldots, e_n) = \det(\mathrm{tr}_{K/F}(e_i e_j)_{1 \le i,j \le n}) \in \mathfrak{o}_F\ .$$

(b) Use part (a) to show that K/F is unramified (that is, if $e_{K/F} = 1$) if and only if $\Delta_{K/F}$ is a unit in $\mathfrak{o}_F$. [*Hint*: Show that the discriminant is a unit in $\mathfrak{o}_F$ if and only if its image in $\mathfrak{o}_F/\pi_F\mathfrak{o}_F$ is nonzero, and that this in turn occurs if and only if $\mathfrak{o}_K/\pi_F\mathfrak{o}_K$ is a field. Then apply Corollary 4-26.]

(c) One says that K/F is *tamely ramified* if the residual characteristic p does not divide $e(K/F)$. Show that K/F is tamely ramified if and only if $v_K(\mathfrak{D}_{K/F})$ (this is the exponent d occurring in the definition of the different) is precisely $e(K/F)-1$. [*Hint*: Show that these conditions are equivalent to having $\mathfrak{o}_F=\mathrm{tr}_{K/F}(\mathfrak{o}_K)$.]

(d) Let L/K also be finite separable extension. Show that

$$\mathfrak{D}_{L/F} = (\mathfrak{D}_{L/K})(\mathfrak{D}_{K/F}\,\mathfrak{o}_L)$$

and that

$$\Delta_{L/F} = N_{K/F}(\Delta_{L/K})\Delta_{K/F}^{[L:K]}\,.$$

14. Let K/F be a finite separable extension of global fields. The *inverse different* of K over F is defined by

$$\mathfrak{D}_{K/F}^{-1} = \{x \in K : \mathrm{tr}_{K/F}(x\mathfrak{o}_K) \subseteq \mathfrak{o}_F\}.$$

This is a fractional ideal of K, whence we set $\mathfrak{D}_{K/F}$, the *different* of K over F, to be its inverse fractional ideal. (Again see Appendix B, both for a discussion of fractional ideals and for a more general treatment of the notions under discussion here.) Define the *discriminant* $\Delta_{K/F}$ to be the ideal of $\mathfrak{o}_F$ generated by $N_{K/F}(\mathfrak{D}_{K/F})$.

REMARK. As above, we abbreviate the notation for the different and the discriminant to $\mathfrak{D}_K$ and Δ_K, respectively, when F is a prime global field. Moreover, in the case of a number field we write d_K for the integer defined up to sign by $\Delta_K=d_K\mathbf{Z}$ and loosely refer to this number as the discriminant.

(a) Show that $\mathfrak{D}_{K/F}^{-1}$ is the largest fractional ideal J of K such that $\mathrm{tr}_{K/F}(J)\subseteq\mathfrak{o}_F$.

(b) Prove the final part of the previous exercise in this global setting.

(c) Let P be a prime ideal in $\mathfrak{o}_F$. Show that

$$\Delta_{K/F}\mathfrak{o}_{F_P} = \prod_{Q|P} \Delta_{K_Q/F_P}$$

where the product is taken over the primes of $\mathfrak{o}_K$ that lie above P. Conclude that P is unramified in K if and only if it does not divide $\Delta_{K/F}$.

(d) Suppose that $\mathfrak{o}_F$ is a principal ideal domain. Show, as in part (a) of the previous exercise, that

$$\Delta_{K/F} = \Delta_{K/F}(e_1, \ldots, e_n)\, \mathfrak{o}_F$$

where $\{e_j\}_{j \leq n}$ is an $\mathfrak{o}_F$-basis for $\mathfrak{o}_K$. If $\mathfrak{o}_F = \mathbf{Z}$, show that $\Delta_K = \Delta_{K/F}(e_1, \ldots, e_n)$ is independent of the choice of $\mathfrak{o}_F$-basis.

(e) Show that every finite extension K of $\mathbf{Q}$ must be ramified at some prime p. [*Hint*: Use the previous two parts.]

15. In light of the previous exercises, we shall now examine cyclotomic extensions.

(a) Let $K = \mathbf{Q}[e^{2\pi i/p^n}]$. Show that $\mathbf{Z}[e^{2\pi i/p^n}]$ is the ring of integers in K.

(b) Let K be as above. With the Δ_K as in the fourth part of the previous exercise, show that

$$\Delta_K = (-1)^r p^{p^{n-1}((p-1)n-1)} \quad \text{where } r = \begin{cases} 1 & \text{if } p^n = 4 \text{ or } p^n \equiv 3 \bmod 4 \\ 0 & \text{otherwise.} \end{cases}$$

[*Hint*: Use Exercise 13 and evaluate

$$\det\left(e^{2\pi i k m/p^n}\right)_{0 \leq k \leq (p-1)p^{n-1},\ m \in (\mathbf{Z}/p^n\mathbf{Z})^\times}$$

the so-called Vandermonde determinant.]

(c) For $m \geq 1$, let $K_m = \mathbf{Q}[e^{2\pi i/m}]$, and let Δ_m denote the corresponding discriminant. Show that if m and r are relatively prime integers, then

$$\Delta_{mr} = \Delta_m \Delta_r .$$

Conclude that the ring of integers in K_m is $\mathbf{Z}[e^{2\pi i/m}]$.

(d) With K_m as above, show that for any $m \geq 1$, the prime p ramifies in K_m if and only if $p \mid m$.

5
Adeles, Ideles, and the Class Groups

To do harmonic analysis on a global field F, one needs to introduce two locally compact abelian groups: $\mathbf{A}_F$, the adele group, and $\mathbf{I}_F$, the idele group. From one perspective, if we view F as a discrete group, it is of great interest to determine its Pontryagin dual $\hat{F}$, which we know must be compact. Recall that for the particular discrete group $\mathbf{Z}$, its dual is simply the quotient $\mathbf{R}/\mathbf{Z}$. We shall see in our analysis that the adele group plays the role of $\mathbf{R}$, in the sense that F naturally embeds discretely in $\mathbf{A}_F$ with compact quotient $\mathbf{A}_F/F$, which ultimately can be identified with $\hat{F}$. For $F=\mathbf{Q}$, one has a canonical surjection $\mathbf{A}_\mathbf{Q}\to\mathbf{R}$, which induces a covering map $\mathbf{A}_\mathbf{Q}/\mathbf{Q}\to\mathbf{R}/\mathbf{Z}$ with totally disconnected fibers. This is discussed, after some preliminaries on approximations, in Section 5.3.

The adele group of a global field F, which is moreover a topological ring, is defined as the "restricted direct product" of the additive groups of the various local completions F_v. The restriction is that an element (x_v) of $\mathbf{A}_F$ must satisfy the condition that almost all of its coordinates x_v lie in the ring $\mathfrak{o}_v$ of integers of F_v, for v finite. The notion of a restricted direct product is in fact more general, as developed in Section 5.1, and applies again when the additive group is replaced by the multiplicative group, leading to the construction of $\mathbf{I}_F$, the idele group. This was first introduced by C. Chevalley as a generalization of the notion of an ideal in F. It turns out that F^* embeds discretely in $\mathbf{I}_F$, but is not cocompact. The quotient $C_F=\mathbf{I}_F/F^*$ is called the *idele class group* of F. We shall see in Section 5.4 that there exists an important compact abelian group C_F^1 such that C_F is isomorphic as a topological group to $C_F^1\times\mathbf{R}_+^\times$ if F has characteristic zero, and to $C_F^1\times\mathbf{Z}$ if F has positive characteristic. Moreover, the classical ideal class group and the ray class group relative to an ideal reveal themselves to be quotients of C_F.

From the vantage point of number theory, the role of $\mathbf{A}_F$ and $\mathbf{I}_F$, at least initially, was to provide an efficient derivation of the classical results of algebraic number theory, as we shall now see. We discuss its further impact on class field theory in Chapter 6. The important later work of Tate, building on the work of Matchett, expanded this role immeasurably, and entered—at the suggestion of E. Artin—analytic number theory as well. Suddenly there surfaced a radical new way to derive Hecke's results on a class of zeta functions, and it led to an

explicit formula for the "root number" occurring in their functional equations. These issues are fully dealt with in Chapter 7.

In many modern applications not discussed in this book, one replaces the multiplicative group of $\mathbf{A}_F$ with $G(\mathbf{A}_F)$, where G is a general "reductive" matrix group such as GL_n. The groups $G(\mathbf{A}_F)$ are locally compact, and the quotients $G(F)\backslash G(\mathbf{A}_F)$ are important homogeneous spaces. If Z denotes the center of G, then $X_F=G(F)Z(\mathbf{A}_F)\backslash G(\mathbf{A}_F)$ has finite volume, and the harmonic analysis on $L^2(X_F)$ relative to the right action of $G(\mathbf{A}_F)$ holds the key, according to the general philosophy of Langlands, to understanding the nonabelian extensions of F.

5.1 Restricted Direct Products, Characters, and Measures

Let $J=\{v\}$ be a set of indices, and let J_∞ be a fixed finite subset of J. Assume that for every index v we are given a locally compact group G_v, not necessarily abelian, and that for all $v\notin J_\infty$, we are further given a compact open (hence closed) subgroup H_v of G_v.

DEFINITION. We define the *restricted direct product* of the G_v with respect to the H_v as follows:

$$\prod_{v\in J}{}' G_v = \{(x_v) : x_v \in G_v \text{ with } x_v \in H_v \text{ for all but finitely many } v\} .$$

Note that the H_v are concealed in this notation; this will cause no confusion.

Let G denote the restricted direct product of the G_v with respect to the H_v. Clearly G is a subset of the ordinary set-theoretic direct product of the G_v and, moreover, a subgroup of the group-theoretic direct product. (In fact, G lies between the direct product and the direct sum of the component groups.)

We define a topology on G by specifying a neighborhood base of the identity consisting of sets of the form $\prod N_v$ where N_v is a neighborhood of 1 in G_v and $N_v=H_v$ for all but finitely many v. Note that this topology is *not* the product topology; it is best understood in terms of the following construction.

Let S be any finite subset of J that contains J_∞, and consider the subgroup G_S of G defined by

$$G_S = \prod_{v\in S} G_v \times \prod_{v\notin S} H_v .$$

Then G_S is the product of a finite family of locally compact groups with a compact group; hence G_S is locally compact in the product topology. Now here is the key point: *the product topology on G_S is identical to that induced by the*

topology defined in the previous paragraph. Hence each subgroup of the form G_S is locally compact with respect to the topology of the restricted direct product. Since every $x \in G$ belongs to some subgroup of this form, it follows at once that G is locally compact.

One verifies at once that G is a topological group with respect to the indicated group structure and topology. Hence we have proven the first part of the following result:

5-1 PROPOSITION. *Let G_v and H_v be as above, and let G be the restricted direct product of the G_v with respect to the H_v. Then*

(i) *G is a locally compact group.*

(ii) *A subset Y of G has compact closure if and only if $Y \subseteq \prod K_v$ for some family of compact subsets $K_v \subseteq G_v$ such that $K_v = H_v$ for all but finitely many indices v.*

PROOF. As noted, we need only argue the second part. Suppose that K, the closure of Y, is a compact subset of G. Since subsets of the form G_S cover G and since subsets of this form are clearly open, a finite number of G_S cover K. But a finite union of G_S is obviously contained in a single subset of this form, whence we conclude that $K \subseteq G_{S_0}$ for some finite collection of indices S_0. From this we can draw two conclusions:

(a) Let ρ_v denote the projection from G onto G_v. Since the topology of G induces the product topology on G_{S_0}, each map ρ_v is continuous. Hence $\rho_v(K)$ is compact for all v.

(b) $\rho_v(K) \subseteq H_v$ for all but finitely many v.

It follows at once that K, and hence Y, is contained in a product $\prod K_v$ of the required form. The converse is obvious. ❑

Finally, note that for each v we have a topological embedding

$$\begin{aligned} G_v &\to G \\ x &\mapsto (\ldots,1,1,1,\underset{\substack{\uparrow \\ v\text{th component}}}{x},1,1,1,\ldots)\ . \end{aligned}$$

Since the image of G_v under this embedding evidently lies in $G_{\{v\}}$, which enjoys the topology of pointwise convergence, it follows that each G_v may be identified with a closed subgroup of G.

Characters

The material in the remainder of this section, while logically belonging to the current discussion, will not be used until Chapter 7. Since our immediate concern is with characters, in this subsection we restrict our attention to abelian groups.

Assume that G is the restricted direct product of the locally compact abelian groups G_v with respect to the open subgroups H_v. As usual, if $y\in G$, we write y_v for the projection of y onto the factor G_v and, as addressed above, we identify G_v with a closed subgroup of G.

5-2 LEMMA. *Let $\chi\in\mathrm{Hom}_{\mathrm{cont}}(G,\mathbf{C}^*)$. Then χ is trivial on all but finitely many H_v. Consequently, for $y\in G$, $\chi(y_v)=1$ for all but finitely many v, and*

$$\chi(y)=\prod_v \chi(y_v)\ .$$

PROOF. We can obviously choose a neighborhood U of 1 in $\mathbf{C}^*$ such that U contains no subgroups of $\mathbf{C}^*$ other than the trivial subgroup. Let $N=\prod N_v$ be an open neighborhood of the identity of G such that $\chi(N)\subseteq U$, with $N_v=H_v$ for all v lying outside some finite subset S of the full index set. Then

$$\prod_{v\notin S} H_v \subseteq N$$

whence

$$\chi(\prod_{v\notin S} H_v)\subseteq U\ .$$

But the left-hand side is a subgroup of $\mathbf{C}^*$, and so

$$\chi(\prod_{v\notin S} H_v)=\{1\}\ .$$

In particular, $\chi(H_v)=\{1\}$ for all $v\notin S$. Now given $y\in G$, we can factor it into a product $y_1y_2y_3$ where

y_1 is the finite product of the projections of y that lie outside of any H_v;

y_2 is the finite product of the projections of y that lie in some H_v for v a member of the index set S identified above;

y_3 comprises the remaining projections of y, all of which lie in some H_v for v *not* lying in S.

This shows that χ is trivial on all but finitely many projections of y; the product formula follows at once. ❑

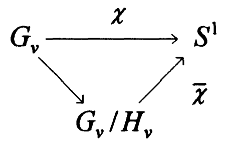
5-3 LEMMA. *For each v let χ_v lie in* $\mathrm{Hom}_{\mathrm{cont}}(G_v, \mathbf{C}^*)$ *and assume that* $\chi_v|_{H_v}=1$ *for all but finitely many v. Then* $\chi=\prod\chi_v$ *lies in* $\mathrm{Hom}_{\mathrm{cont}}(G, \mathbf{C}^*)$.

PROOF. Let S be a finite set of indices such that $\chi_v|_{H_v}=1$ for $v\notin S$, and let m be the cardinality of S. As in the previous proof, $\chi=\prod\chi_v$ is well-defined (i.e., amounts to a finite product), and thus the only issue is continuity. Let U be a neighborhood of 1 in $\mathbf{C}^*$. Choose a second neighborhood V such that $V^{(m)}\subseteq U$. For each $v\in S$ there is a neighborhood N_v of the identity of G_v such that $\chi_v(N_v)\subseteq V$. It follows that

$$\prod_{v\in S} N_v \times \prod_{v\notin S} H_v$$

is a neighborhood of the identity in G that lies in the inverse image of U under χ. Hence χ is continuous, as required. ❑

Given an arbitrary G_v, as usual we can form its dual group $\hat{G}_v$. If moreover, $v\notin J_\infty$, then define $K(G_v,H_v)$ to be the subgroup of characters on G_v that restrict to the trivial map on H_v. Recalling from Section 3.1 the construction of the compact open topology on the dual group, we see that if U is a sufficiently small neighborhood of $1\in S^1$, then, as above, $K(G_v,H_v)=W(H_v,U)$. (The point again is to choose U so small that it contains no nontrivial subgroups of $\mathbf{C}^*$.) Hence $K(G_v,H_v)$ is at least open in $\hat{G}_v$. Now let $\chi\in K(G_v,H_v)$, and consider the following commutative diagram:



This shows that the assignment $\chi\mapsto\bar{\chi}$ defines a mapping from $K(G_v,H_v)$ to $(G_v/H_v)^\wedge$. One shows easily that this is in fact an isomorphism of topological groups. Since H_v is open in G_v, it follows that G_v/H_v is discrete, and hence $(G_v/H_v)^\wedge$ is compact. Thus $K(G_v,H_v)$ is likewise compact, and it makes sense to form the restricted direct product of the groups $\hat{G}_v$ with respect to the subgroups $K(G_v,H_v)$.

5-4 THEOREM. *Let G_v, H_v be as above, and let G be the restricted direct product of the G_v with respect to the H_v. Then as topological groups,*

$$\hat{G}\cong\prod{}'\hat{G}_v$$

where the restricted direct product on the right is taken with respect to the subgroups $K(G_v, H_v)$ defined above.

PROOF. Consider the mapping

$$\begin{aligned} \prod{}' \hat{G}_v &\stackrel{\varphi}{\to} \hat{G} \\ (\chi_v) &\mapsto \prod \chi_v \ . \end{aligned}$$

In view of the two previous lemmas, this is clearly an isomorphism of abstract groups. Hence it remains to show that φ is bicontinuous, and for this it is enough to establish bicontinuity at the identity.

Let U be a neighborhood of 1 in $\mathbf{C}^*$ and let K be a compact neighborhood of the identity of G. We know that $K=\prod K_v$, where K_v is a compact neighborhood of the identity of G_v and $K_v=H_v$ for all but finitely many indices v. A character χ on G lies in the open neighborhood $W(K, U)$ of the trivial character if and only if $\chi(K)=\prod\chi(K_v)\subseteq U$. Suppose that the subset S of indices for which χ is nontrivial on K_v has cardinality m. As previously, we can find a neighborhood V of 1 in $\mathbf{C}^*$ such that $V^{(m)}\subseteq U$. Then if

$$(\chi_v) \in N = \prod_{v \in S} W(K_v, V) \times \prod_{v \notin S} K(G_v, H_v)$$

it follows at once that $\varphi(\chi_v)\in W(K, U)$. But since by definition of the restricted direct product topology N is an open neighborhood of the identity in its ambient group, φ is continuous.

Finally, with the notation as above, let $N=\prod W(K_v, U)$ be an open neighborhood of the identity in the restricted product $\prod' \hat{G}_v$. Then clearly $W(\prod K_v, U)$ is contained in $\varphi(N)$, and hence φ is open as well as continuous. ❑

Measures

We shall now show how to define measures on restricted direct products of locally compact groups and, in the abelian case, on their Pontryagin duals.

5-5 PROPOSITION. *Let $G=\prod'_{v\in J} G_v$ be the restricted direct product of locally compact groups G_v with respect to the family of compact subgroups $H_v\subseteq G_v$ (for $v\notin J_\infty$). Let dg_v denote the corresponding (left) Haar measure on G_v normalized so that*

$$\int_{H_v} dg_v = 1$$

for almost all $v \notin J_\infty$. Then there is a unique Haar measure dg on G such that for each finite set of indices S containing J_∞, the restriction dg_S of dg to

$$G_S = \prod_{v \in S} G_v \times \prod_{v \notin S} H_v$$

is precisely the product measure.

Proof. Choose a set S as indicated and define a measure dg_S by taking the product of the measures dg_v. The normalization of these measures forces the volume of the compact group $\Pi_{v \notin S} H_v$ to be finite, as needed, and one checks easily that dg_S is indeed a Haar measure on G_S. Suppose now that $T \supseteq S$ is a larger finite set of indices. Then, of course,

$$G_S = (\prod_{v \in S} G_v \times \prod_{v \in T-S} H_v) \times (\prod_{v \notin T} H_v) \subseteq (\prod_{v \in S} G_v \times \prod_{v \in T-S} G_v) \times (\prod_{v \notin T} H_v) = G_T \ .$$

Moreover, by construction,

$$dg_S = (\prod_{v \in S} dg_v \times \prod_{v \in T-S} dg_v) \times (\prod_{v \notin T} dg_v)$$

and

$$dg_T = (\prod_{v \in S} dg_v \times \prod_{v \in T-S} dg_v) \times (\prod_{v \notin T} dg_v) \ .$$

We conclude at once from this that dg_S coincides with the restriction of dg_T to the subgroup G_S.

Now, since G is locally compact, we know it has a Haar measure, which restricts to a Haar measure on any G_S. Accordingly, we may fix *any* set S of indices containing J_∞, and define a Haar measure dg on G to be *the* Haar measure that restricts to dg_S. That this measure is independent of S and unique follows from the conclusion of the first paragraph: given two sets of indices S and S', the measure dg constructed relative to S uniquely picks out the product measure on $G_{S \cup S'}$ and hence also on $G_{S'}$. ❑

Henceforth we write

$$dg = \prod_v dg_v$$

for the (left) Haar measure on G defined by the proposition. We refer to this as the measure *induced* by the factor measures. We shall next learn how to integrate nice functions on G relative to dg.

5-6 PROPOSITION. *Let G be a restricted direct product of locally compact groups as above, with induced measure dg.*

(i) *Let f be an integrable function on G. Then*

$$\int_G f(g)dg = \lim_S \int_{G_S} f(g_S)dg_S .$$

If f is only assumed to be continuous, this formal identity still holds, provided that we allow the indicated integral to assume infinite values.

(ii) *Let S_0 denote any finite set of indices including J_∞ and those v for which* $\mathrm{Vol}(H_v, dg_v) \neq 1$, *and suppose that for each index v we are given a continuous integrable function f_v on G_v such that $f_v|_{H_v}=1$ for all $v \notin S_0$. For $g=(g_v) \in G$, define*

$$f(g) = \prod_v f_v(g_v) .$$

Then f is well-defined and continuous on G. If S is any finite set of indices including S_0, we have

$$\int_{G_S} f(g_S)dg_S = \prod_{v \in S} \Big(\int_{G_v} f_v(g_v)dg_v \Big) . \tag{5.1}$$

Moreover,

$$\int_G f(g)dg = \prod_v \Big(\int_{G_v} f_v(g_v)dg_v \Big)$$

and $f \in L^1(G)$, provided that the right-hand product is finite.

(iii) *Let $\{f_v\}$ and f be as in the previous part, with the added condition that f_v is the characteristic function of H_v for almost all v. Then f is integrable. Moreover, in the abelian case, the Fourier transform of f is likewise integrable and in fact given by*

$$\hat{f}_v(g) = \prod_v \hat{f}_v(g_v) . \tag{5.2}$$

PROOF. (i) Certainly

$$\int_G f(g)dg = \lim_C \int_C f(g)dg$$

where the limit is taken over compact subsets C of G. But any such C is contained in some G_S, and the limit formula follows. Clearly, the identity holds formally for f continuous, but not necessarily integrable.

(ii) Since $f_v|_{H_v}=1$ for almost all v and since $g=(g_v)\in G$ has (by definition) almost all of its components g_v in H_v, $\prod f_v(g_v)$ is in fact a finite product for all such g, and f is well-defined. The continuity of f follows easily from the continuity of each f_v because a base for G can be given in the form $\prod N_v \times \prod H_v$, where the first factor is a finite product containing all of the components of G on which the corresponding function f_v is nontrivial. Hence f may be computed locally as a finite product of continuous functions.

Now fix any S satisfying the hypothesis of part (ii). Then by the definition of G_S and the assumption that $f_v|_{H_v}=1$ and $\mathrm{Vol}(H_v, dg_v)=1$ for all v not in S, it is clear that Eq. 5.1 holds since dg_S is precisely the product measure on G_S. To prove the second statement, note that by part (i), f is integrable if and only if

$$\lim_S \int_{G_S} f(g_S)dg_S < \infty$$

where the limit is taken over larger and larger S. But Eq. 5.1 implies that this limit exists if and only if

$$\lim_S \prod_{v\in S} \Big(\int_{G_v} f_v(g_v)dg_v\Big) = \prod_{\text{all } v} \Big(\int_{G_v} f_v(g_v)dg_v\Big) < \infty$$

which is true by hypothesis.

(iii) Since f_v is the characteristic function of H_v for almost all v,

$$\prod_{v} \Big(\int_{G_v} f_v(g_v)dg_v\Big) = \prod_{v\in S} \Big(\int_{G_v} f_v(g_v)dg_v\Big)$$

for some finite set S, and is hence convergent. Therefore f is integrable on G.

In the abelian case, to establish the assertions about the Fourier transform, let $\chi=(\chi_v)$ denote a character of G, and for each f_v, define h_v to be the product $f_v\chi_v$. Define h as $\prod_v h_v$. Then h is integrable, since χ is unitary, and the assertions of part (ii) applied to h immediately yield Eq. 5.2. ❑

Assume henceforth that our groups are abelian. The final goal of this section is to build a product measure on the group

$$\hat{G} = \prod_{v}{}' \hat{G}_v$$

that is dual to $dg = \prod_v dg_v$ in the sense defined by the Fourier inversion theorem (Theorem 3-9), where we again assume that the measures dg_v have been normalized so that H_v has volume 1 for almost all v. For each v, let

$$d\chi_v = (dg_v)\hat{}$$

denote the dual measure to dg_v on $\hat{G}_v$. For each v and $f \in L^1(G_v)$, we have by definition that

$$\hat{f}_v(\chi_v) = \int_{G_v} f_v(g_v)\overline{\chi}_v(g_v)dg_v \ .$$

If f_v is the characteristic function of H_v, which is clearly integrable and of positive type on G_v, we deduce from the orthogonality relations that in fact

$$\hat{f}_v(\chi_v) = \int_{H_v} \chi_v(g_v)dg_v = \begin{cases} \mathrm{Vol}(H_v) & \text{if } \chi_v|_{H_v} = 1 \\ 0 & \text{otherwise.} \end{cases}$$

In other words, if H_v^* is the subgroup of $\hat{G}_v$ consisting of characters trivial on H_v [that is, what we have previously denoted $K(G_v, H_v)$], then $\hat{f}_v(\chi_v)$ is the characteristic function of H_v^* times the volume of H_v. From this observation and the Fourier inversion formula, it follows that

$$\mathrm{Vol}(H_v)\mathrm{Vol}(H_v^*) = 1$$

where the first volume is computed relative to dg_v and the second relative to $d\chi_v$. Consequently the latter measure also gives volume 1 to H_v^* for almost all v, and we can define $d\chi = (dg)\hat{}$ as above.

5-7 Proposition. *The measure $d\chi$ so defined is dual to dg. That is,*

$$f(g) = \int_{\hat{G}} \hat{f}(\chi)\chi(g)d\chi$$

for all $f \in V^1(G)$.

PROOF. Since we seek only to determine a normalization factor, it suffices to check the formula given above for the product functions $f=\prod f_v$ with f_v equal to the characteristic function of H_v for almost all v. The left hand-side is $\prod f_v(g_v)$, while according to the previous proposition, the right-hand side is

$$\prod_v \int_{\hat{G}_v} \hat{f}_v(\chi_v)\chi_v(g_v)d\chi_v \ .$$

But since $d\chi_v$ is the dual measure to dg_v,

$$f_v(g_v) = \int_{\hat{G}_v} \hat{f}_v(\chi_v)\chi_v(g_v)d\chi_v$$

for each v, and the assertion follows. ❑

5.2 Adeles, Ideles, and the Approximation Theorem

Let K be a global field and let K_v be the completion of K at a place v. Then $\langle K_v,+\rangle$ is a locally compact additive group, which in the case of an algebraic number field is either $\mathbf{R}$, $\mathbf{C}$, or a $\mathfrak{p}$-adic field. For all finite places v, K_v admits $\mathfrak{o}_v$ as an open compact subgroup. The restricted direct product of the K_v over all v with respect to the subgroups $\mathfrak{o}_v$ (v finite) is called the *adele group* of K and denoted $\mathbf{A}_K$. Note that we have an algebraic embedding

$$\begin{aligned} K &\rightarrow \mathbf{A}_K \\ x &\mapsto (x,x,x,\ldots) \ . \end{aligned}$$

This map is well-defined because K always embeds in K_v for all absolute values v and every element of K is a local integer for all but finitely many places.

Along the same lines, for all places v of K, we can consider the locally compact multiplicative groups $\langle K_v^*, \cdot \rangle$. Here the local units $\mathfrak{o}_v^\times$ (v finite) constitute an open compact subgroup, and hence we may form the restricted direct product of the K_v^* with respect to the subgroups $\mathfrak{o}_v^\times$. This is called the *idele group* of K and denoted $\mathbf{I}_K$. Again we have an algebraic embedding

$$\begin{aligned} K^* &\rightarrow \mathbf{I}_K \\ x &\mapsto (x,x,x,\ldots) \end{aligned}$$

which is clearly well-defined.

REMARK. The adele group $\mathbf{A}_K$ admits an obvious ring structure, and we have an algebraic isomorphism $\mathbf{I}_K \cong \mathbf{A}_K^\times$ that identifies the idele group with a subset of

the adele group. However, this is *not* a topological embedding: the topology on the idele group as a restricted direct product is in fact stronger than the relative topology induced by the full adele group. We can see this easily in the case $K=\mathbf{Q}$. Let S be any finite collection of primes including the infinite prime, and let N_p be any neighborhood of 1 in $\mathbf{Q}_p$ for $p\in S$. Then

$$\Big(\prod_{p\in S} N_p \times \prod_{p\notin S} \mathbf{Z}_p\Big)\cap \mathbf{I}_{\mathbf{Q}} \not\subset \mathbf{R}^* \times \prod_{p<\infty} \mathbf{Z}_p^{\times} .$$

The point is that we can construct a point $x=(x_p)$ in the product appearing on the left such that for some $p\notin S$, x_p is a p-adic integer but not a p-adic unit; this does not exclude x from $\mathbf{I}_{\mathbf{Q}}$, but it does exclude it from the open set displayed on the right. Hence the neighborhood base of the relative topology on $\mathbf{I}_{\mathbf{Q}}$ induced from the adele group cannot in general accommodate the open sets in the idele topology, which consequently is stronger. (We leave it to the reader to observe that every set open in the relative topology is also open in the idele topology.) Despite this dissonance, these topologies are related by an algebraic map, as shown in Exercise 1.

Fix K and let S_ω denote the set of infinite places of K. Note that $S_\omega=S_\infty$ in characteristic zero. We write $\mathbf{A}_\omega$ for the open subgroup $\mathbf{A}_{S_\omega}$ of the adele group $\mathbf{A}_K$. Hence $\mathbf{A}_\omega$ consists of elements of the adele group all of whose components at finite places have absolute value less than or equal to one.

5-8 THEOREM. (The Approximation Theorem) *For every global field K,*

$$\mathbf{A}_K = K + \mathbf{A}_\omega \ .$$

Moreover, $K\cap\mathbf{A}_\omega = \mathfrak{o}_K$.

PROOF. Here, of course, we identify K with the diagonal subset of its adele group. We must show that given $x\in\mathbf{A}_K$, there exists $\mu\in K$ such that each component of the difference $x-\mu$ is a local integer. We give the argument for K an algebraic number field; the modifications for a function field are obvious.

Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}_K$ and assume that $\mathfrak{p}$ lies over the rational prime p. Then multiplying any nonzero element of the associated completion by p certainly reduces its $\mathfrak{p}$-adic absolute value, so that eventually it lies in the corresponding ring of integers. This shows that there exists some finite rational integer m such that mx is integral at all finite primes. Let $\{\mathfrak{p}_1,\ldots,\mathfrak{p}_r\}$ be the set of primes of K that divide m (clearly this set must include all the primes at which the corresponding component of x fails to be integral), and let $n_1,\ldots,n_r$ be a sequence in $\mathbf{N}$. By the Chinese remainder theorem (see Exercise 2 below), we can find $\lambda\in\mathfrak{o}_K$ such that

$$mx_j \equiv \lambda \pmod{\mathfrak{p}_j^{n_j}}$$

where x_j is the component of the adele x corresponding to $\mathfrak{p}_j$. Let $\mu=\lambda/m$. If we choose each n_j at least as large as the exponent of $\mathfrak{p}_j$ occurring in the factorization of the ideal (m) in $\mathfrak{o}_K$, then $x-\mu=m^{-1}(mx-\lambda)$ is by construction integral at each of the primes $\mathfrak{p}_1,\ldots,\mathfrak{p}_r$. At other primes, its absolute value is identical to that of $mx-\lambda$, and hence it remains integral. This establishes the first assertion; the second is trivial. ❑

5-9 COROLLARY. *Let* $\mathbf{A}$ *denote the adele group of* $\mathbf{Q}$. *Then*

$$\mathbf{A} = \mathbf{Q} + \mathbf{A}_\infty = \mathbf{Q} + (\mathbf{R} \times \prod_{p \text{ prime}} \mathbf{Z}_p) .$$

Moreover, $\mathbf{Q} \cap \mathbf{A}_\infty = \mathbf{Z}$. ❑

5.3 The Geometry of $\mathbf{A}_K/K$

Let K denote a global field. Before describing the structure of the quotient of $\mathbf{A}_K$ by K, we must first investigate how the adeles behave under base change.

5-10 LEMMA. *Let* E/K *be a finite extension, and fix a K-basis* $\{u_1,\ldots,u_n\}$ *of* E. *Then the natural map*

$$\alpha : \prod_{j=1}^{n} \mathbf{A}_K \to \mathbf{A}_E$$
$$((x_{v,j})_v)_j \mapsto \sum_j u_j (x_{v,j})_v$$

is an isomorphism of topological groups.

PROOF. The map α is certainly a vector space isomorphism, so the question is only one of continuity. For every place v of K, define

$$E_v = \prod_{w|v} E_w$$

where w runs through the places of E lying above v. This is, of course, not a field, but certainly a vector space over K_v, in which K_v itself embeds diagonally. We have shown in Section 4.5 (Proposition 4-39) that E_v admits $\{u_1,\ldots,u_n\}$ as a K_v-basis, and thus an algebra isomorphism

$$\alpha_v : \prod_{j=1}^{n} K_v \xrightarrow{\sim} E_v$$
$$(x_j) \mapsto \sum x_j u_j \ .$$

By Proposition 4-13, α_v is also a topological isomorphism.

Define a subset $\mathfrak{o}_{E_v}$ of E_v by

$$\mathfrak{o}_{E_v} = \prod_{w|v} \mathfrak{o}_{E_w} \ .$$

Then again by Proposition 4-39 there exists a finite set of places S_0 of K, including the Archimedean ones, such that for every $v \notin S_0$ the map α_v defined above induces by restriction an isomorphism

$$\alpha_v : \prod_{j=1}^{n} \mathfrak{o}_{K_v} \xrightarrow{\sim} \mathfrak{o}_{E_v} \ .$$

Now for any given finite set S that contains S_0, consider the products

$$\mathbf{A}_K^S = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathfrak{o}_{K_v} \quad \text{and} \quad \mathbf{A}_E^S = \prod_{v \in S} E_v \times \prod_{v \notin S} \mathfrak{o}_{E_v} \ .$$

Then from what we have seen so far,

$$\prod_{j=1}^{n} \mathbf{A}_K^S = \prod_{j=1}^{n} \Big(\prod_{v \in S} K_v \times \prod_{v \notin S} \mathfrak{o}_{K_v} \Big) \cong \prod_{v \in S} E_v \times \prod_{v \notin S} \mathfrak{o}_{E_v} = \mathbf{A}_E^S \ .$$

Thus for each such set of places S, the collection $\{\alpha_v\}$ induces a map

$$\alpha^S : \prod_{j=1}^{n} \mathbf{A}_K^S \xrightarrow{\sim} \mathbf{A}_E^S$$

which, according to the analysis of the previous paragraph, is a topological isomorphism and by construction agrees with the restriction of α. Since this is true for every S containing S_0 and the open sets $\mathbf{A}_E^S$ cover $\mathbf{A}_E$, we deduce that α itself must be a topological isomorphism. ❑

5-11 THEOREM. *K is a discrete, cocompact subgroup of $\mathbf{A}_K$.*

PROOF. Let K_0 denote $\mathbf{Q}$ [respectively, the function field $\mathbf{F}_q(t)$] if K is of characteristic zero [respectively, of characteristic p]. Put $n=[K:K_0]$. Then by the preceding lemma we have the following commutative diagram of topological groups, for which the top and bottom rows are isomorphisms:

$$\begin{array}{ccc} \prod_{j=1}^{n} \mathbf{A}_{K_0} & \xrightarrow{\ \alpha\ } & \mathbf{A}_K \\ \uparrow & & \uparrow \\ \prod_{j=1}^{n} K_0 & \xrightarrow{\ \alpha| \ } & K \end{array}$$

Consequently, $\mathbf{A}_K/K$ is compact if and only if $(\mathbf{A}_{K_0}/K_0)^n$ is compact, which in turn is true if and only if $\mathbf{A}_{K_0}/K_0$ is compact; similarly for discreteness. Thus we may replace K by K_0 and assume for the remainder of the proof that K is either $\mathbf{Q}$ or $\mathbf{F}_q(t)$. In the former case, let ∞ denote the Archimedean place; in the latter case, let ∞ denote the place defined by (t^{-1}). Put $\mathfrak{o}_K$ equal to $\mathbf{Z}$ or $\mathbf{F}_q[t]$, accordingly. We shall now exhibit a compact fundamental domain for K in $\mathbf{A}_K$.

Define a subset C of the adele group by

$$C=\{x\in\mathbf{A}_K : |x_\infty|_\infty \le \tfrac{1}{2} \text{ and } |x_v|_v \le 1 \ \forall v\ne\infty\} \ .$$

It now suffices to show that $C\cap K=\{0\}$ and that $\mathbf{A}_K=C+K$.

Suppose that $x\in K$ also lies in C. Then $x\in\mathfrak{o}_K$, since $x\in\mathfrak{o}_v$ for all $v\ne\infty$. In the rational case, the requirement that $|x_\infty|_\infty\le 1/2$ certainly forces x to be zero. Now consider the function field case. Then

$$|x|_\infty = q^{-\operatorname{ord}_{1/t}(x)}$$

which cannot be less than $1/2$ for nonzero elements of $\mathbf{F}_q[t]$. This shows that indeed $C\cap K=\{0\}$.

It remains to show that $\mathbf{A}_K$ is covered by translates of K by elements in C, and we do this in two steps. First we claim that if y is an adele of K, then we may choose $\delta\in K$ such that $y_v-\delta\in\mathfrak{o}_v$ for every finite place v of K. We only need to worry about a finite set S of places, and for each $v\in S$, we may construct an element $\mu=\mu(v)\in K$ such that $y-\mu$ is integral at v, and μ is integral at all finite places different from v. To see this we need merely note that for any irreducible element π in $\mathfrak{o}_K$, positive n, and integral elements a and b relatively prime to π, we can always find a third integral element c such that

$$\frac{a}{b\pi^n} - \frac{c}{\pi^n}$$

is integral at π, because the congruence $a \equiv bc \pmod{\pi^n}$ is clearly solvable for c. Thus $\delta = \sum_{v\in S}\mu(v)$ meets our needs, and this completes the first step.

Continuing with y and δ as above, we claim that we can next choose $\delta' \in \mathfrak{o}_K$ such that $|y_\infty - \delta - \delta'|_\infty \leq 1/2$. If $K=\mathbf{Q}$, the number δ' is just the integer nearest to $(y_\infty - \delta)$; if $K=\mathbf{F}_q(t)$, then δ' is just the part of $(y_\infty - \delta)$ that is a polynomial in t. (The remainder is a polynomial in t^{-1} with no constant term, and hence of infinity norm less than q^{-1}, a value patently less than or equal to 1/2.) Now by construction, both $(y_v - \delta)$ and δ' lie in $\mathfrak{o}_v$ for all finite places v. Thus

$$|y_v - \delta - \delta'|_v \leq 1 \quad \textit{and} \quad |y_\infty - \delta - \delta'|_\infty \leq 1/2$$

whence $x = y - \delta - \delta' \in C$. This clearly suffices, since by construction, $x + \delta + \delta' = y$ and $\delta + \delta' \in K$. □

If K is a number field, then the preceding result is the adelic version of the well-known fact that $\mathfrak{o}_K$ is a discrete, cocompact subgroup of $K_\infty = \prod K_w$, where the product is taken over all Archimedean w. Moreover, in the case $K=\mathbf{Q}$ we can apply the approximation theorem to yield the following beautiful description of the quotient of $\mathbf{A_Q}$ by $\mathbf{Q}$.

5-12 PROPOSITION. *There exists an isomorphism of topological groups*

$$\mathbf{A_Q}/\mathbf{Q} \xrightarrow{\sim} \varprojlim \mathbf{R}/n\mathbf{Z} \ .$$

The projective limit is, of course, taken over the positive integers as a directed set with respect to divisibility.

PROOF. For each positive integer n set

$$C_n = \{x \in \mathbf{A_Q} \colon x_\infty = 0 \text{ and } x_p \in p^{\operatorname{ord}_p(n)}\mathbf{Z}_p \text{ for } p < \infty\} \ .$$

Clearly each C_n is a compact subgroup, and moreover, the intersection of the C_n over all n is $\{0\}$. This yields an identification

$$\begin{aligned} \varprojlim \mathbf{A_Q}/C_n &\xrightarrow{\sim} \mathbf{A_Q} \\ ((\bar{x}_{p,n})_p)_n &\mapsto (\lim_n x_{p,n})_p \end{aligned}$$

where the ordinary limit on the right is also taken over the positive integers as a directed set with respect to divisibility. (The point is that if we fix a prime p, the sequence that results from taking the pth components of the indexed set of adeles that constitute an element of the projective limit must converge in $\mathbf{Q}_p$.) This isomorphism in turn induces an identification of quotients

$$\mathbf{A}_\mathbf{Q}/\mathbf{Q} \cong \varprojlim \mathbf{A}_\mathbf{Q}/(\mathbf{Q}+C_n) \ .$$

Now consider the map

$$\varphi_n : \mathbf{R}/n\mathbf{Z} \to \mathbf{A}_\mathbf{Q}/(\mathbf{Q}+C_n)$$

given by sending x to the class of the adele with x as the Archimedean component and zero as the finite component. This map is well-defined, because for all products na, $a \in \mathbf{Z}$, we have the decomposition

$$\underset{\substack{\uparrow\ \uparrow\ \uparrow \\ \infty\ 2\ 3}}{(na,0,0,\ldots)} = (na, na, na, \ldots) + (0, -na, -na, \ldots) \in \mathbf{Q}+C_n \ .$$

It is immediate that φ_n is injective. The surjectivity follows from the approximation theorem, the proof of which may be readily extended to show that the finite part of $\mathbf{A}_\infty$ may in fact be replaced by C_n. From the existence of these isomorphisms φ_n, we now deduce that

$$\mathbf{A}_\mathbf{Q}/\mathbf{Q} \cong \varprojlim \mathbf{A}_\mathbf{Q}/(\mathbf{Q}+C_n) \cong \varprojlim \mathbf{R}/n\mathbf{Z}$$

and this completes the proof. ❑

REMARK. Thus $\mathbf{A}_\mathbf{Q}/\mathbf{Q}$ is an inverse limit whose nth component corresponds to the unique covering of $\mathbf{R}/\mathbf{Z}$ of degree n, $n \geq 1$. Since $\pi_1(\mathbf{R}/\mathbf{Z}) = \mathbf{Z}$ has $\mathbf{Z}/n\mathbf{Z}$ as its unique quotient of order n for each $n \geq 1$, every finite cover of S^1 is obtained from $\mathbf{A}_\mathbf{Q}/\mathbf{Q}$. Thus $\mathbf{A}_\mathbf{Q}/\mathbf{Q}$ may be thought of as the "algebraic universal covering space" of S^1, analogous to $\mathbf{R}$ as the "topological universal covering space" of S^1. The Galois group of the covering $\mathbf{A}_\mathbf{Q}/\mathbf{Q} \to S^1$, namely $\hat{\mathbf{Z}}$, may be thought of as the "algebraic fundamental group" of S^1. This is a simple instance of Grothendieck's general construction of the algebraic fundamental group for algebraic varieties, a notion that arose in connection with the following situation: Let X be a smooth projective algebraic curve over $\mathbf{C}$, so that the set of complex points $X(\mathbf{C})$ defines a Riemann surface; i.e., a complex manifold of dimension 1. Suppose that Y is a finite covering of $X(\mathbf{C})$. Then by the Riemann existence theorem, Y corresponds to a smooth projective algebraic curve X' with

$Y=X'(\mathbf{C})$. But if Y is an infinite cover, it will not be algebraic, and therefore one needs to restrict to finite covers to remain in the algebraic category.

5.4 The Class Groups

In this section, we reverse the historical order and begin with the definition of the *idele class group* C_K of a global field K. We analyze its properties and then show how the usual ideal class group Cl_K and, more generally, any ray class group relative to an ideal, is a factor of the compact part of C_K. (In the function field case, the class group Cl_K is usually called the *Picard group* and denoted $\operatorname{Pic} \mathfrak{o}_K$.)

Let K be an algebraic number field or a finitely generated function field in one variable over a finite field $\mathbf{F}_q$ where $q=p^a$. Just as K embeds discretely in $\mathbf{A}_K$, K^* identifies with a discrete subgroup of the idele group $\mathbf{I}_K$ via the diagonal map. (See Exercise 3.) Since $\mathbf{I}_K$ is abelian, its quotient by K^* under the quotient topology acquires the structure of a topological group [cf. Proposition 1-4, (v)].

DEFINITION. The topological group

$$C_K = \mathbf{I}_K/K^*$$

is called the *idele class group* of K.

Since $\mathbf{A}_K/K$ is compact, one might hope that C_K is also compact. But this is not true, as follows from the existence of a nontrivial absolute value that will be defined shortly. But first we must standardize our absolute value functions:

DEFINITION. Let k be a local field. Then the *normalized* absolute value $|\cdot|_k$ on k is defined as follows:

(i) If $k=\mathbf{R}$, then $|\cdot|_k$ is the usual absolute value function.

(ii) If $k=\mathbf{C}$, then $|z|_k=z\bar{z}$, the square of the usual absolute value function.

(iii) If k is non-Archimedean with uniformizing parameter π, then

$$|\pi|_k=\frac{1}{q}$$

where q is the order of the residue field $\mathfrak{o}_k/\pi\cdot\mathfrak{o}_k$. This clearly extends uniquely to k. Note well that for the infinite place associated with a function field of positive characteristic in the indeterminate t (so that the uniformizing parameter is in fact t^{-1}), this normalized absolute value function amounts to the formula $|f(t)|_\infty=q^{\deg f}$ for polynomials $f(t)$. (Hence the infi-

nite place described in Chapter 4 was represented precisely by the corresponding normalized absolute value function.)

The following lemma shows how these normalized absolute values behave with respect to finite extensions of local fields. Recall that if l/k is a finite extension of arbitrary fields, then every element $x \in l$ defines, by multiplication, an endomorphism ρ_x of l as a vector space over k; this is just the regular representation. In this context, the norm of x over k, denoted $N_{l/k}(x)$, is the determinant of ρ_x. For a Galois extension, this reduces to the product of the conjugates of x; in any case, $N_{l/k}$ is multiplicative.

5-13 LEMMA. *Let l/k be a finite extension of local fields. Then for all $x \in E$, we have*

$$|x|_l = |N_{l/k}(x)|_k \ .$$

PROOF. This is clear in the Archimedean cases. So let k be non-Archimedean with uniformizing parameter π_k. It suffices to prove the lemma for $x = \pi_l$, the uniformizing parameter for l. Let $n = [l:k]$. Recall from Proposition 4-23 that the ramification index and residual degree for the extension are defined by the relations

$$\pi_k = u\pi_l^e \quad (u \in \mathfrak{o}_l^\times)$$

$$q^f = \mathrm{Card}(\mathfrak{o}_l / \pi_l \cdot \mathfrak{o}_l)$$

and that $n = ef$. We may certainly replace π_k with $u^{-1}\pi_k$, so that $\pi_k = \pi_l^e$. Accordingly,

$$N_{l/k}(\pi_l^e) = \pi_k^n$$

and it follows that

$$|N_{l/k}(\pi_l^e)|_k = \frac{1}{q^{ef}} \ .$$

Thus taking eth roots of this equation and recalling the definition of $|\cdot|_l$, we obtain

$$|\pi_l|_l = \frac{1}{q^f} = |N_{l/k}(\pi_l)|_k$$

as required. ❑

We now apply our construction of normalized absolute values to make the following definition. Again let K be global field.

DEFINITION. Let $|\cdot|_v$ denote the normalized absolute value on the completion K_v. Then define the absolute value $|\cdot|_{\mathbf{A}_K}:\mathbf{I}_K\to\mathbf{R}_+^*$ by the formula

$$|x|_{\mathbf{A}_K}=\prod_v |x_v|_v$$

where as usual, $x=(x_v)$.

CRUCIAL REMARK. From the analysis of local fields in Chapter 4, it follows that for any idele x, the value of $|x|_{\mathbf{A}_K}$ is precisely the module of the automorphism $y\mapsto xy$ as defined on the locally compact abelian group $\mathbf{A}_K$. (See the discussion preceding Proposition 4-17.) This explains the choice of normalization at the non-Archimedean places and, moreover, why the normalized absolute value on $\mathbf{C}$ has been chosen as the square of the usual absolute value.

5-14 THEOREM. *Let K be a global field. Then*

(i) *For every $x\in K^*$ we have $|x|_{\mathbf{A}_K}=1$.*

(ii) *The absolute value map $|\cdot|_{\mathbf{A}_K}$ is surjective if* $\mathrm{char}(K)=0$ *and has image of the form $p^{m_0\mathbf{Z}}$ if* $\mathrm{char}(K)=p$, *where m_0 is an integer different from* 0.

The first part of this result is known as *Artin's product formula*.

PROOF. (i) Suppose that E/K is a finite separable extension. Then according to the lemma, for every $x\in E$, we may write

$$\begin{aligned}|x|_{\mathbf{A}_E}&=\prod_{u\in\mathcal{P}_K}\ \prod_{v\in\mathcal{P}_E,v|u}|x|_v\\&=\prod_{u\in\mathcal{P}_K}\ \prod_{v\in\mathcal{P}_E,v|u}|N_{E_v/K_u}(x)|_u\ .\end{aligned}$$

But appealing to the isomorphism of Proposition 4-40, $E\otimes_K K_u\cong\prod_{v|u}E_v$, we see that

$$\prod_{v|u}N_{E_v/K_u}(x)=N_{E/K}(x)\ \ .$$

Thus

$$|x|_{\mathbf{A}_E} = \prod_u |N_{E/K}(x)|_u$$

and so the truth of the assertion for K will imply it for E. Since we have shown that every global field is a finite separable extension of either $\mathbf{Q}$ or $\mathbf{F}_q(t)$, we have now reduced the argument to these two cases. Moreover, since $|\cdot|_{\mathbf{A}_K}$ is multiplicative, it suffices to establish the product formula for integral irreducibles.

Suppose that $K=\mathbf{Q}$ and p is a rational prime. We may take p to be positive, since it is clear that $|-1|_v=1$ for all v. Then p has nontrivial absolute value at only two places and hence

$$|p|_{\mathbf{A}_K} = |p|_\infty \cdot |p|_p = p \cdot p^{-1} = 1 \ .$$

This establishes the product formula for $\mathbf{Q}$. For $K=\mathbf{F}_q(t)$, we must consider an irreducible polynomial $f(t)\in\mathbf{F}_q[t]$, and again this has nontrivial absolute value at only two places. For the infinite place,

$$|f(t)|_\infty = q^{\deg f}$$

as noted above, while at the finite place,

$$|f(t)|_f = q^{-\deg f}$$

since of course, $\mathrm{Card}(\mathbf{F}_q[t]/f(t)\mathbf{F}_q[t])$ is $q^{\deg f}$. Thus once more the product formula holds.

(ii) First assume that K is a number field, so that there is at least one Archimedean place w. For any positive real number t, we can pick some $y\in K_w^*$ such that $|y|_w=t$. Let x denote the idele whose w-component is y with all other components equal to 1. Clearly, $|x|_{\mathbf{A}_K}=|y|_w=t$, whence $|\cdot|_{\mathbf{A}_K}$ is surjective.

Next let K be a function field over a finite field, and let v be a place of K with corresponding residue field $\mathbf{F}_q$, where $q=p^m$. Then the normalized absolute value of a uniformizing parameter π of K_v is q^{-1}. Accordingly, given $n\in\mathbf{Z}$, the absolute value of the idele $x=(1,\ldots,1,\pi^{-n},1,\ldots)$ is p^{mn}. The upshot is that the image of each component of $\mathbf{A}_K$ under the adelic absolute value is $p^{m\mathbf{Z}}$, and hence the total image is $p^{m_0\mathbf{Z}}$ for some nonzero integer m_0. This completes the proof. ❑

We next use the absolute value $|\cdot|_{\mathbf{A}_K}$ on $\mathbf{A}_K$ to define a subgroup of $\mathbf{I}_K$ into which K^* does embed cocompactly. The key is to trivialize the absolute value.

Definition. Let K be an algebraic number field or a finitely generated function field in one variable over a finite field $\mathbf{F}_q$, where $q=p^a$. Then we define

$$\mathbf{I}_K^1 = \mathrm{Ker}(|\cdot|_{\mathbf{A}_K})$$

(the ideles of norm one) and

$$C_K^1 = \mathbf{I}_K^1 / K^* \ .$$

This quotient is called the *norm-one idele class group* of K.

Note that C_K^1 is well-defined, since $K^* \subseteq \mathbf{I}_K^1$ by the Artin product formula. Moreover, we have a short exact sequence

$$1 \to C_K^1 \to C_K \to V(\mathbf{I}_K) \to 1$$

where according to the characteristic of K, $V(\mathbf{I}_K) = \mathrm{Im}(|\cdot|_{\mathbf{A}_K})$ is either $\mathbf{R}_+^*$ or of the form $p^{m_0\mathbf{Z}}$.

5-15 THEOREM. *For all global fields K, the quotient*

$$C_K^1 = \mathbf{I}_K^1 / K^*$$

is compact.

PROOF. Recall from the proof of Theorem 5-11 that there is a compact subset Φ of $\mathbf{A}_K$ such that $\mathbf{A}_K = K + \Phi$. Since $\mathbf{A}_K$ is locally compact, there exists a Haar measure μ on $\mathbf{A}_K$, which we shall now fix; of course, $\mu(\Phi)$ is finite. Choose a compact subset Z of $\mathbf{A}_K$ such that $\mu(Z) > \mu(\Phi)$. Construct two subsets of differences and products of elements in Z as follows:

$$Z_1 = \{z_1 - z_2 : z_1, z_2 \in Z\}$$

$$Z_2 = \{z_1 z_2 : z_1, z_2 \in Z\}$$

These sets are also compact by the continuity of subtraction and multiplication. Since K is discrete in $\mathbf{A}_K$, $K \cap Z_2$ is finite, with *nonzero* elements, say, $y_1, \ldots, y_r$. Now set

$$\Psi = \bigcup_{j=1}^{r} \delta^{-1}(\{(u, y_j^{-1} v) : u, v \in Z_1\})$$

where δ is the embedding of $\mathbf{I}_K$ into $\mathbf{A}_K \times \mathbf{A}_K$ that sends x to (x, x^{-1}). (See Exercise 1.) Since δ is a homeomorphism onto its image, Ψ is a compact subset of $\mathbf{I}_K$, whence the theorem is a consequence of the following claim:

CLAIM. $\mathbf{I}_K^1 \subseteq K^*\Psi$.

PROOF OF CLAIM. First recall that for any $y\in\mathbf{I}_K$, $|y|_{\mathbf{A}_K}=\Pi_v|y_v|_v$ is the module of the automorphism of $\mathbf{A}_K$ given by multiplication by y. Now pick any $x\in\mathbf{I}_K^1$. Since $|x|_{\mathbf{A}_K}=1$, we see that the compact sets xZ and $x^{-1}Z$ have the same volume as Z. Since $\mu(Z)>\mu(\Phi)$, it follows from Exercise 4 that there exist elements $z_1,z_2,z_3,z_4\in Z$, $z_1\neq z_2$, $z_3\neq z_4$, such that $\alpha=x(z_1-z_2)$ and $\beta=x^{-1}(z_3-z_4)$ are both in K. Then $\alpha\beta=(z_1-z_2)(z_3-z_4)$ evidently belongs to $K^*\cap Z_2=\{y_1,\ldots,y_r\}$. In other words, $(z_1-z_2)(z_3-z_4)\,y_j^{-1}=1$, for some $j\leq r$. Thus

$$\delta(x\beta)=\delta(z_3-z_4)=(z_3-z_4,\,(z_1-z_2)y_j^{-1})\in Z_1\times Z_1y_j^{-1}\ .$$

This shows that $x\beta\in\Psi$ and completes the proof. ❑

It is useful to have S-versions of the groups we have been discussing, for any finite set S of places of K containing S_∞, the set of Archimedean places. Of course, there are no such Archimedean places if char$K$ is positive. (This notation is unfortunately conventional, although not entirely sensible: it *excludes* the infinite places for a function field. Let the reader beware.)

DEFINITION. Let K and $S\supseteq S_\infty$ be as above. Then define the *S-ideles* of K by

$$\mathbf{I}_{K,S}=\{x=(x_v)\in\mathbf{I}_K : x_v\in\mathfrak{o}_v^\times, \forall v\notin S\}\ .$$

Equivalently,

$$\mathbf{I}_{K,S}=\prod_{v\in S}K_v^*\times\prod_{v\notin S}\mathfrak{o}_v^\times\ .$$

5-16 LEMMA. $\mathbf{I}_{K,S}$ *is open in* $\mathbf{I}_K$; *it is compact if and only if* $S=\varnothing$, *which can occur only in positive characteristic.*

PROOF. That $\mathbf{I}_{K,S}$ is open in $\mathbf{I}_K$ is clear, because the restricted direct product topology on $\mathbf{I}_K$ is the same as the relative topology induced by the product $\Pi_vK_v^*$. (See Section 5.1.) Since K_v^* is not compact for any v, $\mathbf{I}_{K,S}$ is compact if and only if S is empty. But in characteristic zero, we require that S contain the nonempty set of Archimedean places, so this can happen only in positive characteristic, as claimed. ❑

DEFINITION. Let K and $S\supseteq S_\infty$ be as above. Then

$$\mathbf{I}_{K,S}^1=\mathbf{I}_K^1\cap\mathbf{I}_{K,S}$$

denotes the set of *S-ideles of norm one.*

According to the lemma, $\mathbf{I}^1_{K,S}$ is an open subgroup of $\mathbf{I}^1_K$ in the relative topology induced by the full idele group.

DEFINITION. The *ring of S-integers* of K is defined to be

$$R_S = K \cap \mathbf{A}_{K,S}$$

where

$$\mathbf{A}_{K,S} = \{x \in \mathbf{A}_K : x_v \in \mathfrak{o}_v,\ \forall v \notin S\} \ .$$

The definition above in particular gives $\mathfrak{o}_K$ as R_{S_∞} for K a number field, and $\mathfrak{o}_K$ as R_{S_0} for K a function field, where in the latter case S_0 denotes the set of infinite places of K. Also note that

$$R_S^\times = K^* \cap \mathbf{I}_{K,S} = K^* \cap \mathbf{I}^1_{K,S} \ .$$

This is because $\mathbf{I}_{K,S}$ is the group of invertible elements in $\mathbf{A}_{K,S}$ and

$$\mathbf{A}_{K,S} = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathfrak{o}_v \ .$$

5-17 PROPOSITION. *Let S be a finite set of places of K containing S_∞. The following statements hold:*

(i) *The quotient $\mathbf{I}^1_{K,S}/R_S^\times$ is compact.*

(ii) *There exists an isomorphism*

$$R_S^\times \cong \mu_K \times \mathbf{Z}^{r(S)}$$

where μ_K is the group of roots of unity in K and

$$r(S) = \sup\{0, \mathrm{Card}(S) - 1\} \ .$$

PROOF. (i) Since $\mathbf{I}^1_{K,S}$ is open in $\mathbf{I}^1_K$, its image $\mathbf{I}^1_{K,S}/R_S^\times$ is an open (hence closed) subgroup of $\mathbf{I}^1_K/K^*$. But according to our previous theorem, the ambient space is compact, and hence the assertion.

(ii) Since we know this for the special case $S = \varnothing$ (see Exercise 5), we may assume that S is nonempty. Put

$$C=\prod_v C_v$$

where the product is taken over all places and $C_v=\{x_v \in K_v : |x_v|_v=1\}$. This "adelic circle" is a compact subgroup of $\mathbf{I}_{K,S}$. We have a short exact sequence of topological groups

$$1 \to C \to \mathbf{I}_{K,S} \to \prod_{v \in S} (K_v^*/C_v) \to 1 \ .$$

Note that

$$K_v^* / C_v \cong \begin{cases} \mathbf{R}_+^\times \overset{\log}{\cong} \mathbf{R}, & \text{if } v \text{ is Archimedean} \\ \mathbf{Z}, & \text{if } v \text{ is non-Archimedean.} \end{cases}$$

Writing $r=r_1+r_2$, where r_1 is the number of Archimedean places in S and r_2 is the remainder, this yields the sequence

$$1 \to C \to \mathbf{I}_{K,S}^1 \to \mathbf{R}^{r_1} \times \mathbf{Z}^{r_2} \ .$$

Since, again by Exercise 5, $C \cap K^* = \mu_K$ and also $\mathbf{I}_{K,S}^1 \cap K^* = R_S^\times$, we get the short exact sequence

$$1 \to \mu_K \to R_S^\times \to L \to 1$$

where L is the image of K^* in $\mathbf{R}^{r_1} \times \mathbf{Z}^{r_2}$. Since K^* is discrete and cocompact in $\mathbf{I}_{K,S}^1$, an application of Exercise 6 below (with $\lambda=\prod|\cdot|_v$) shows that L is isomorphic to $\mathbf{Z}^{r(S)}$. ❑

REMARK. Part (i) implies in particular that R_S^* is finitely generated as an abelian group, a fact that is not obvious from the definition. For K a number field and $S=S_\infty$, this was established by Dirichlet and Minkowski.

We now introduce S-versions of the idele class group, which have a critical property when S is nonempty.

DEFINITION. The *S-class group* of K is defined by

$$C_{K,S} = \mathbf{I}_K/(K^* \cdot \mathbf{I}_{K,S}) \ .$$

The critical property is this: The inclusion map of norm-1 ideles into the full idele group always induces an injection of quotients

$$\mathbf{I}_K^1/K^*\mathbf{I}_{K,S}^1 \to \mathbf{I}_K/K^*\mathbf{I}_{K,S} \quad .$$

However, if $S\neq\varnothing$, this map is moreover an isomorphism, because we can then always represent any idele class on the right with an idele of norm one by adjusting a component corresponding to a place in S. If S is empty, then we are in characteristic $p>0$, and the map has cokernel isomorphic to $\mathbf{Z}$ by Theorem 5-14, part (ii).

5-18 THEOREM. *The S-class groups of K have the following properties:*

(i) *In the case that S is nonempty,* $\mathrm{C}_{K,S}$ *is a finite group.*

(ii) *In the case that S is empty,* $C_{K,\varnothing}$ *is isomorphic to the direct product of* $\mathbf{Z}$ *with a finite group.*

PROOF. We have seen that the image of $\mathbf{I}_{K,S}^1$ in $\mathbf{I}_K^1$ is open. Since $\mathbf{I}_K^1/K^*$ is compact, the quotient $\mathbf{I}_K^1/K^*\mathbf{I}_{K,S}^1$ must then be finite. The theorem now follows from the preceding analysis of the injection of $\mathbf{I}_K^1/K^*\mathbf{I}_{K,S}^1$ into $\mathrm{C}_{K,S}$. ❑

The Traditional Class Group

A global field K is the field of fractions of the Dedekind domain $R=\mathfrak{o}_K$, the ring of integers of K. A *fractional ideal* of K is a nonzero finitely generated R-submodule of K. Thus in particular, the ordinary nonzero ideals of R are fractional ideals of K. One knows from the basic theory of Dedekind domains that J_K, the set of fractional ideals of K, constitutes a group under multiplication of (fractional) ideals and, moreover, that J_K is a free abelian group on the prime ideals of R. This is to say that we may write every fractional ideal $\mathfrak{a}\in J_K$ *uniquely* as

$$\mathfrak{a} = \prod_P P^{n_P}$$

where the product is taken over all prime ideals P of R and n_P is zero for almost all P. (See Appendix B.) We sometimes write $v_P(\mathfrak{a})$ for the exponent n_P defined by this factorization, and similarly define $v_P(x)$ for nonzero $x\in K$. More precisely, $v_P(x)=v_P(xR)=\mathrm{ord}_\pi(x)$, where π is a uniformizing parameter for R_P. We call v_P the *discrete valuation* associated with P.

Fractional ideals of the form $R\alpha$, $\alpha\in K^*$, are called *principal fractional ideals*, and these constitute a subgroup P_K of J_K that includes the nonzero principal

ideals of R. The quotient group J_K/P_K is the traditional *ideal class group* of K, here denoted Cl_K. If $\mathfrak{a}\in J_K$, then $[\mathfrak{a}]$ denotes its projection into the class group.

As previously, S_ω denotes the set of infinite places of a global field K. Hence S_ω is either S_∞ for a number field or S_0 for a function field.

5-19 PROPOSITION. *Let K be a global field. Then there is a natural isomorphism*

$$C_{K,S_\omega} \cong Cl_K \ .$$

PROOF. Define a map

$$\begin{aligned} \tilde{\alpha} : \mathbf{I}_K &\to Cl_K \\ x &\mapsto [\prod_P P^{v_P(x_P)}] \end{aligned}$$

with v_P as above. Then $\tilde{\alpha}$ is a well-defined homomorphism. Moreover, if $x\in K^*$, then

$$(x) = \prod_P P^{v_P(x)}$$

is the principal fractional ideal generated by x, and so $\tilde{\alpha}(x)=1$. Since $\tilde{\alpha}(x)$ depends only on the components of x corresponding to the finite places, $\tilde{\alpha}$ is trivial on $\Pi_{(v\in S_\omega)}K_v^*$. Finally, $\tilde{\alpha}$ is trivial on $\Pi_P\, \mathfrak{o}_P^\times$, since $\mathfrak{o}_P^\times\subseteq\mathrm{Ker}(v_P)$ for all P. In summary, $\tilde{\alpha}$ is trivial on $K^*\mathbf{I}_{K,S_\omega}$ and hence induces a homomorphism

$$\alpha : C_{K,S_\infty} \to Cl_K$$

sending the class of x to $\tilde{\alpha}(x)$.

Suppose that $\mathfrak{a}\in J_K$. Then $v_P(\mathfrak{a})$ is nonzero for only a finite number of P. Accordingly, we may define an idele x by requiring that x be nonzero at the infinite places and $x_P=\pi_P^{v_P(\mathfrak{a})}$ for the places corresponding to primes P, where π_P is the associated uniformizing parameter. Then by construction $\alpha([x])=[\mathfrak{a}]$, and thus α is surjective.

Finally, suppose that $\alpha([x])=1$ for some $x\in\mathbf{I}_K$. Then there is a $y\in K^*$ such that

$$(y) = \prod_P P^{v_P(x_P)} \ .$$

This implies that for all P, $v_P(y)=v_P(x_P)$, and so we may choose $u=(u_P)\in\prod\mathfrak{o}_P^\times$ such that $(xu)_P=y_P$, for all P. Then xu and y differ by an element of $\prod_{(v\in S_\omega)}K_v^*$; that is, x and y differ by an element of $\mathbf{I}_{K,S_\omega}$. Consequently, $x\in K^*\cdot\mathbf{I}_{K,S_\omega}$, which means that its class $[x]$ in C_{K,S_ω} is trivial. Hence α is also injective. ❑

REMARK. By saying that α is natural we mean that it is functorial for the inclusion of fields in one direction and for the norm map in the other.

Ray Class Groups

Again let K be a global field, the fraction field of $R=\mathbf{A}_\omega\cap K$, with fractional ideal group J_K. Let M be a nonzero integral ideal of R, so that we may factor M uniquely as

$$M = \prod_{v \text{ finite}} P_v^{v_P(M)}$$

where P_v is the prime corresponding to the finite place v of K, with associated discrete valuation v_P. Let S be the set of finite places where $v_P(M)>0$.

DEFINITION. An element $\alpha\in K^*$ is said to be *congruent to* 1 mod M if the following conditions hold at every $v\in S$:

(i) $\alpha\in \mathfrak{o}_v^\times$

(ii) $v_P(\alpha-1)\geq v_P(M)$

The set of all such α is denoted $K_{M,1}$; one checks easily that this constitutes a subgroup of K^*.

DEFINITION. Let K and M be as above. Then define

$$J_K(M) = \{I\in J_K : (I,M) = R\} \ .$$

That is, $J_K(M)$ consists of the fractional ideals of K that are comaximal with respect to M. In particular, if $\alpha\in K_{M,1}$, then $\alpha R\in J_K(M)$. We may thus further define

$$Cl_K(M) = J_K(M)/K_{M,1} \ .$$

We call $Cl_K(M)$ the *(wide) ray class group of* K relative to M (or with conductor M).

EXAMPLE. Consider the case $K=\mathbf{Q}$. Then $R=\mathbf{Z}$ is a principal ideal domain, $R^\times=\{\pm1\}$, and each nonzero integral ideal M takes the form $m\mathbf{Z}$ for some unique positive integer m. Define a map

$$\varphi : Cl_K(M)\to (\mathbf{Z}/m\mathbf{Z})^\times/\{\pm1\}$$

that sends the class of a fractional ideal $(a/b)\mathbf{Z}$ (with both numerator and denominator prime to m) to the double residue class $\pm[a][b]^{-1}$. This map is well-defined on $J_K(M)$ and factors through $Cl_K(M)$ because $(a/b)\mathbf{Z}$ maps to the identity if and only if $a \equiv \pm b \pmod{m}$ in the elementary sense. Since φ is clearly surjective, it is in fact and isomorphism.

More generally, for a number field K this construction is usually extended to include the signs at the real places. Let $\{w_1,\ldots,w_l\}$ be a set of real embeddings representing inequivalent real places (not necessarily exhaustive), and put

$$\tilde{M} = (M, w_1, \ldots, w_l)$$

where M is an integral ideal.

DEFINITION. An element $\alpha \in K^*$ is said to be *congruent to* 1 mod $\tilde{M}$ if the following conditions hold at every $v \in S$:

(i) $\alpha \equiv 1 \pmod{M}$, as above

(ii) $w_j(\alpha) > 0$, $\forall j = 1, \ldots, l$

The set of all such α is denoted $K_{\tilde{M},1}$, and as previously, this constitutes a subgroup of K^*.

DEFINITION. We define the quotient

$$Cl_K(\tilde{M}) = J_K(M) / K_{\tilde{M},1} \ .$$

When $\{w_1,\ldots,w_l\}$ comprises the entire set of real places of K, then this is called the *narrow ray class group of* K relative to M.

EXAMPLE CONTINUED. Again consider the case $K=\mathbf{Q}$. Let $\tilde{M} = (M, \infty)$, with M generated by $m>0$ as before. We can now in a sense refine our map φ to an isomorphism

$$Cl_K(\tilde{M}) \cong (\mathbf{Z}/m\mathbf{Z})^\times \ .$$

The point is that by using the narrow ray class group, we can distinguish signs in $(\mathbf{Z}/m\mathbf{Z})^\times$. More particularly, given any ideal $x\mathbf{Z}$ in $J_K(M)$, we take $x=a/b$, with a and b uniquely given positive integers relatively prime to m and to each other, and then map $x\mathbf{Z}$ to $[a][b]^{-1}$. This map is clearly a surjective homomorphism with kernel $K_{\tilde{M},1}$.

Exercises

1. Let K be a global field, and let $\mathbf{A}_K^2$ have the product topology. Show that the mapping

$$\begin{aligned} \mathbf{I}_K &\to \mathbf{A}_K^2 \\ x &\mapsto (x, x^{-1}) \end{aligned}$$

is a topological isomorphism onto its image (under the relative topology induced by that of the codomain).

2. Let A be an integral domain for which all prime ideals are maximal. Show that if P_1 and P_2 are distinct prime ideals of A, then

$$P_1^m + P_2^n = A$$

for all positive integers m and n. [*Hint*: Prove this directly for all m when $n=1$, and then proceed by induction.]

3. Let K be a global field. Use the discrete embedding of K into the associated adele group and Exercise 1 to show that K^* embeds discretely in the associated idele group.

4. Let G be a locally compact abelian group with Haar measure μ. Suppose that Γ is a subgroup of G and that Φ is a compact subset of G such that $G=\Gamma+\Phi$. Show that if X is a compact subset of G such that $\mu(X)>\mu(\Phi)$, then there exist distinct elements $x_1, x_2 \in X$ such that $x_1 - x_2 \in \Gamma$.

5. Let K be a global field. Show that $|x|_v=1$ at every place v of K if and only if x is a root of unity in K.

6. Let G be a topological group isomorphic to $\mathbf{R}^r \times \mathbf{Z}^{s+1-r}$ for some integers $s \geq r \geq 0$, and let $\lambda: G \to \mathbf{R}$ be a nontrivial, continuous homomorphism such that when $r>0$, λ is in particular nontrivial on $\mathbf{R}^r$. Assume that Γ is a discrete, cocompact subgroup of $\mathrm{Ker}(\lambda)$. Show that $\Gamma \cong \mathbf{Z}^s$.

7. Let K be a global field. Show that the isomorphism $\alpha: C_{K,S_\infty} \cong Cl_K$ is natural in the sense of the remark following Proposition 5-19.

8. Let K be a global field and let S be a finite, nonempty set of places of K containing the infinite ones. Show that R_S [$=K \cap \mathbf{A}_{K,S}$), the ring of S-integers of K, is a Dedekind domain. [*Hint*: Appeal to the case $S=S_\infty$, where we know this to be true by Appendix B.]

9. For any Dedekind domain R with fraction field K, define $\mathrm{Pic}(R)$ to be the group of invertible fractional ideals of K modulo the principal ones. With this definition and the preceding exercise in mind, prove the following S-version of Proposition 5-19:

Let K be a global field, and let S be a finite nonempty set of places of K containing the infinite ones. Then there is an isomorphism $C_{K,S} \cong \mathrm{Pic}(R_S)$.

Show also that for S large enough, $C_{K,S}$ is trivial.

10. Let K be a number field.

(a) Show that an element $x \in K^*$ is a unit of $\mathfrak{o}_K$ if and only if $\mathrm{N}_{K/\mathbf{Q}}(x) = \pm 1$.

Assume for the remainder of this exercise that K is a *quadratic number field*; that is, $K = \mathbf{Q}(\delta)$, where $\delta^2 = d$, a square-free integer.

(b) Show that

$$\mathfrak{o}_K = \begin{cases} \mathbf{Z}[\delta] & \text{if } d \equiv 2,3 \pmod 4 \\ \mathbf{Z}[\frac{1+\delta}{2}] & \text{if } d \equiv 1 \pmod 4). \end{cases}$$

(c) Assuming that d is negative, list the units of $\mathfrak{o}_K$.

(d) Assuming that d is positive and congruent to either 2 or 3 modulo 4, show that the units of $\mathfrak{o}_K$ are precisely those numbers $a+b\delta$ such that the integer pair (a,b) satisfies Pell's equation $a^2 - db^2 = \pm 1$. Show, moreover, that there is a *fundamental unit* $u_1 = a_1 + b_1\delta$, $a_1, b_1 > 0$, such that every unit in $\mathfrak{o}_K$ is of the form $\pm u_1^n$ for some $n \in \mathbf{Z}$. The pair (a_1, b_1) is called a *fundamental solution* to Pell's equation.

(e) For this part, we assume that the reader is familiar with continued fractions. Assume that d is as in the previous part, and let $[a_0, a_1, \ldots, a_n, \ldots]$ be the (simple) continued fraction expansion of δ with "convergents"

$$A_n/B_n = [a_0, a_1, \ldots, a_n] .$$

Show that for some n, the pair (A_n, B_n) constitutes a fundamental solution to Pell's equation. Check in particular that when $d=2$ (respectively, 3), the fundamental unit of $K=\mathbf{Q}(\delta)$ is $1+\delta$ (respectively, $5+2\delta$).

11. Let R be a Dedekind domain, for example the ring of integers in a number field.

(a) Suppose that Pic(R), the class group of the fraction field of R, is trivial. Show then that R is a unique factorization domain; that is, every nonzero element of R is expressible as the (finite) product of irreducible elements and that this factorization is unique up to order and associates. [*Hint*: Show that any two elements $a, b \in R$, not both zero, have a greatest common divisor by looking at the intersection of aR with bR.]

(b) Show that every integral ideal I in R can be written as the intersection of a finite number of principal ideals.

(c) Prove the converse of part (a): if R is a unique factorization domain, then Pic(R) is trivial. [*Hint*: To show that every integral ideal is principal, show first that having unique factorization forces the intersection of any two principal ideals to be principal, and then appeal to part (b).]

MORAL. The class number h_K of a number field measures the failure of unique factorization in $\mathfrak{o}_K$.

12. (Artin) This exercise develops an explicit description of the connected component of C_K^1. Let K be a number field of degree $n = r_1 + 2r_2$, where r_1 and r_2 are, respectively, the number of real and nonconjugate complex embeddings of K into $\mathbf{C}$. Recalling that $\mathfrak{o}_K^\times$ has rank $r = r_1 + r_2 - 1$, fix a set $\{u_1, \ldots, u_r\}$ of multiplicatively independent units in $\mathfrak{o}_K$. Put

$$V = \mathbf{R} \oplus \hat{\mathbf{Z}}$$

and embed $\mathbf{Z}$ in V by the diagonal map that sends m to (m, m). Write

$$\mathbf{I}_K = \mathbf{I}_K^\infty \times \mathbf{I}_K^f$$

where the elements in $\mathbf{I}_K^\infty$ (respectively, $\mathbf{I}_K^f$) have only trivial finite (respectively, infinite) components.

(a) Show that for any $y \in \mathbf{I}_K^f$ and $x \in \hat{\mathbf{Z}}$, the expression y^x makes sense. [*Hint*: $\mathbf{I}_K^f$ has a fundamental system of neighborhoods of unity consisting of subgroups of finite index.]

(b) Show that for any $z \in \mathbf{I}_K^f$ and $t \in \mathbf{R}$, the expression z^t makes sense, and that it can be normalized to obtain real values at real places.

(c) For $j=1,\ldots,r_2$ and $t\in\mathbf{R}$, let $\phi_j(t)$ denote the idele with component $e^{2\pi i t}$ at the jth complex place and 1 everywhere else. Define a map $\tilde{A}$ by

$$\tilde{A} : V^r \oplus \mathbf{R}^{r_2} \rightarrow \mathbf{I}_K^1$$
$$(\lambda,t)=(\lambda_1,\ldots,\lambda_r;t_1,\ldots t_{r_2}) \mapsto \prod_{i=1}^{r} u_i^{\lambda_i} \prod_{j=1}^{r_2} \phi_j(t_j) \ .$$

Show that $\tilde{A}(\lambda,t)$ is a principal idele if and only if every λ_i and every t_j lies in $\mathbf{Z}$.

(d) Let $A: V^r \oplus \mathbf{R}^{r_2} \rightarrow C_K^1$ denote the induced map to the idele class group. Show that $V/\mathbf{Z}$ is compact, connected, and infinitely and uniquely divisible. Conclude that $D=\operatorname{Im}(A)$ is compact, connected, and infinitely divisible.

(e) Show that every infinitely divisible element of C_K^1 lies in the closure of D, and hence lies in D itself.

(f) Show that D contains the connected component of C_K^1, and conclude that in fact D *is* the connected component of C_K^1. [*Hint*: Use that D contains the image of $\mathbf{I}_K^\infty \cap \mathbf{I}_K^f$.]

13. Let R be a commutative ring with unity. Define the *Heisenberg group* of R as follows:

$$H(R)=\left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in R \right\} \ .$$

Show that for any global field, $H(K)$ embeds as a discrete, cocompact subgroup of $H(\mathbf{A}_K)$.

14. Continuing in the context of the previous problem, show that the abelianization map

$$H(\mathbf{A}_K) \rightarrow \mathbf{A}_K^2$$
$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mapsto (a,b)$$

induces a continuous surjective map

$$\pi\colon H(\mathbf{A}_K)/H(K) \to (\mathbf{A}_K/K)^2$$

whose fibers identify with $\mathbf{A}_K/K$.

15. Let K be a global field.

(a) Show that $\mathrm{GL}_2(K)$ embeds as a discrete subgroup of $\mathrm{GL}_2(\mathbf{A}_K)$.

(b) Show that the corresponding quotient space—not quotient group, for this embedding is not normal—is *not* compact.

(c) Let $Z(\cdot)$ denote the subgroup of $\mathrm{GL}_2(\cdot)$ consisting of scalar matrices. Show that the quotient space $\mathrm{GL}_2(\mathbf{A}_K)/Z(\mathbf{A}_K)\mathrm{GL}_2(K)$ is still not compact.

6
A Quick Tour of Class Field Theory

One could argue that the principal goal of number theory is to understand the integral or rational solutions of systems of Diophantine equations; that is, polynomial equations with integral coefficients. Nineteenth-century mathematicians, mainly riding the impetus provided by attempts to tackle the Fermat equation $x^n+y^n=z^n$ $(n\geq 3)$, realized the benefits of studying the solutions in extended number systems R, as opposed to confining one's attention to only $\mathbf{Z}$ and $\mathbf{Q}$, and this led eventually to global and local fields and their rings of integers. Such an extension often was made to allow for the presence of suitable roots of unity in R, which provided desirable factorizations, such as

$$x^n + y^n = \prod_{j=0}^{n-1} (x + e^{2\pi ij/n} y) \ .$$

Two related problems immediately arose, the first associated with the general failure of unique factorization in R, leading to the class group, and the second pertaining to the question of how rational primes factor, or *split*, in R. The latter problem was first solved in its entirety, in the guise of the study of quadratic forms, for quadratic fields $F=\mathbf{Q}(\delta)$, where $\delta^2=D$ is an integer that is not a square in $\mathbf{Q}$. It was established that an odd prime p splits in F if and only if D is a quadratic residue—that is, a square—mod p, and that the set X_D of primes for which D is a quadratic residue mod p completely determines the extension $F/\mathbf{Q}$. (In modern parlance, one says that the set X_D defines a canonical open subgroup of the idele class group $C_{\mathbf{Q}}$.) Of special importance here is the quadratic reciprocity law, which for primes p and q gives a precise relationship between the status of p as a quadratic residue mod q and the status of q as a quadratic residue mod p. Further progress followed on cyclotomic and Kummer extensions, and, perhaps most significantly, an assertion of Kronecker led to the realization of all abelian extensions of $\mathbf{Q}$ as subextensions of the cyclotomic ones.

By the early twentieth century, the central problem of algebraic number theory had become that of describing the splitting of primes in finite abelian extensions ("class fields") L of an arbitrary number field K in terms of structures associated with K itself. A particular subclass that was well understood

early on was the maximal unramified abelian extension $H(K)$, called the *Hilbert class field* of K, whose Galois group $\mathrm{Gal}(H(K)/K)$ turned out to be isomorphic to the ideal class group Cl_K. In the 1930s, Takagi gave a general solution to the problem and established in the process an abstract isomorphism of the Galois group of any finite abelian extension L of K with a ray class group of K. (As we have seen in Chapter 5, every ray class group is a quotient of the idele class group.) A completely satisfactory understanding of abelian extensions L/K was finally achieved with the revolutionary work of E. Artin, who proved a general reciprocity law. Artin reciprocity, on the one hand, vastly extends Gauss's law of quadratic reciprocity and, on the other, gives a *canonical* isomorphism between $\mathrm{Gal}(L/K)$ and the relevant ray class group. The key tool is a crucial homomorphism called the Artin map.

In this chapter, after introducing the required technical preliminaries on Frobenius elements, the Tchebotarev density theorem—a huge generalization of Dirichlet's theorem on primes in arithmetic progressions—and the transfer map, we summarize (without proof) the main results of abelian class field theory à la Artin. While we state everything for idele class groups rather than ray class groups, the reader may consult Section 5.4 for the relevant dictionary. Putting matters in adelic language might seem an unnecessary complication, but it is absolutely essential if we are to apply the techniques of harmonic analysis. We end the chapter with an explicit description of the abelian extensions of $\mathbf{Q}$ and $\mathbf{Q}_p$, including a proof of the Kronecker-Weber theorem.

SPECIAL NOTES. (i) The results of this chapter are not prerequisite for the proof of Tate's thesis in the following chapter, but they will play a role in some of our applications. (ii) In the exercises for Chapter 7, we shall develop a proof of the Tchebotarev density theorem as reformulated in terms of *Dirichlet density*. Since this proof in fact relies on Artin reciprocity, it is important to stress here that Artin's law is itself independent of the Tchebotarev density theorem. While Artin was inspired by ideas in Tchebotarev's proof, his actual argument does not depend upon it, and hence we introduce no latent circularities.

6.1 Frobenius Elements

The goal of this section is to introduce a family of special elements—or, more properly, of special conjugacy classes—in the Galois groups of global fields. We fix a global field F, and for any Galois extension K/F denote the corresponding Galois group $\mathrm{Gal}(K/F)$.

We shall first consider the case of a *finite* Galois extension K/F with $G=\mathrm{Gal}(K/F)$. Let Q be a prime of $\mathfrak{o}_K$. Then Q lies above some prime P in $\mathfrak{o}_F$, and we let $\mathbf{F}$ denote the residue field $\mathfrak{o}_F/P$. Recall from Section 4.3 that we then define the *decomposition group* of Q in G to be

$$D_Q = \{\sigma \in G : \sigma(Q) = Q\} .$$

Let the residue field $\mathfrak{o}_K/Q$ be identified with the finite field $\mathbf{F}_q$. Then we have a canonical homomorphism

$$\rho_Q : D_Q \to \mathrm{Gal}(\mathbf{F}_q/\mathbf{F})$$

that associates with $\sigma \in D_Q$ the map ($x \bmod Q \mapsto \sigma(x) \bmod Q$) for all $x \in \mathfrak{o}_K$. As proven previously, the map ρ_Q is always surjective and is in fact an isomorphism if and only if P is unramified in K. Moreover, each $\sigma \in D_Q$ extends to an automorphism of the completion K_Q that is trivial on the subfield F_P; the induced map

$$j_Q : D_Q \to \mathrm{Gal}(K_Q/F_P)$$

is unconditionally an isomorphism.

One knows from elementary field theory that $\mathrm{Gal}(\mathbf{F}_q/\mathbf{F})$ is cyclic, generated by the *Frobenius map*

$$x \mapsto x^{p^f}$$

where $\mathrm{Card}(\mathbf{F}) = p^f$. With this in mind, we make the following definition.

DEFINITION. Let P be unramified in K. Then the *Frobenius element* $\varphi_{Q/P}$ in $D_Q \subseteq G$ associated with Q/P is defined by

$$\varphi_{Q/P} = \rho_Q^{-1}(x \mapsto x^{p^f}) .$$

Note that this element unfortunately depends on the choice of Q over P. Indeed, suppose that Q' is another prime dividing P. Note first that $D_{Q'}$ is conjugate to D_Q. Explicitly, we know that we can find $\beta \in G$ such that $\beta(Q') = Q$, and consequently $\beta^{-1}\sigma\beta$ preserves Q' for each $\sigma \in D_Q$.

6-1 LEMMA. *The maps* $\varphi_{Q/P}$ and $\varphi_{Q'/P}$ *are conjugate in the Galois group* G.

PROOF. Choose $\beta \in G$ as above so that $\beta D_{Q'} \beta^{-1} = D_Q$. Then by definition,

$$\varphi_{Q'/P} = \rho_{Q'}^{-1}(x \mapsto x^{p^f}) .$$

To show that this is conjugate by β to $\varphi_{Q/P}$, we explicitly compute as follows:

$$\begin{aligned}\beta^{-1}\varphi_{Q/P}\beta(x+Q') &= \beta^{-1}\varphi_{Q/P}(\beta(x)+Q) \\ &= \beta^{-1}(\beta(x^{p^f})+Q) \\ &= x^{p^f}+Q' \\ &= \varphi_{Q'/P}(x+Q') \ .\end{aligned}$$

This completes the proof. ❑

DEFINITION. The *Frobenius class* in G corresponding to P, denoted $\varphi_{P,K/F}$ or $(P,K/F)$, is the conjugacy class of the Frobenius element $\varphi_{Q/P}$.

This is well-defined by the previous lemma. The notation $(P, K/F)$ is sometimes called the *Artin symbol* of P relative to K/F. We shall next analyze the functorial properties of these Frobenius classes.

6-2 PROPOSITION. *The Artin symbol has the following properties:*

(i) *Let M/F be a finite Galois extension and K/F a normal subextension, so that the restriction map $N_{M/K}$ from* $\mathrm{Gal}(M/F)$ *to* $\mathrm{Gal}(K/F)$ *induces an isomorphism between* $\mathrm{Gal}(M/F)/\mathrm{Gal}(M/K)$ *and* $\mathrm{Gal}(K/F)$. *Then for any prime P unramified in M,*

$$N_{M/K}(P,M/F) = (P,K/F)\ .$$

(ii) *Let K and K' be two finite Galois extensions of F that are, moreover, linearly disjoint over F. Then for every prime P unramified in KK', we have that $\sigma\in\mathrm{Gal}(KK'/F)$ lies in the Frobenius class $(P,KK'/F)$ if and only if $(\sigma|_K, \sigma|_{K'})\in(P,K/F)\times(P,K'/F)$.*

(iii) *Let K/F be a finite Galois extension, and let L be an intermediate field, not necessarily normal over F, with $[K:L]=m$. Let P be a prime of F unramified in K, and suppose that Q is a prime of L that divides P and that $\overline{P}$ is a prime of K that divides Q. Then we have that $L_Q=F_P$ if and only if $\varphi_{\overline{P}/P}\in\mathrm{Gal}(K/L)$. Moreover, the number of primes Q of L lying over P such that $L_Q=F_P$ is given by the formula*

$$\frac{1}{m}\mathrm{Card}\,(\,\{\sigma\in\mathrm{Gal}(K/F):\sigma\varphi_{\overline{P}/P}\sigma^{-1}\in\mathrm{Gal}(K/L)\ \}\,)\,.$$

REMARK. A prime Q of L dividing P such that $L_Q=F_P$ is called a *degree-one* prime over F. When L/F is normal, $(P,K/F)$ is a subset of $\mathrm{Gal}(K/L)$ if and only

if $\varphi_{\overline{P}/P} \in \mathrm{Gal}(K/L)$ for some Frobenius element defined over P, and in this case P splits completely in L into a product of primes of degree 1.

PROOF. (i) Let P' be a prime of K above P, and P'' a prime of M above P'. Let k, k', and k'' denote the corresponding residue fields. Then we have the following diagram:

$$\begin{array}{ccccc} M & \to & M_{P''} \supseteq \mathfrak{o}_{P''} & \to & k'' \\ | & & & & | \\ K & \to & K_{P'} \supseteq \mathfrak{o}_{P'} & \to & k' \\ | & & & & | \\ F & \to & F_P \supseteq \mathfrak{o}_P & \to & k \end{array}$$

Let $k = \mathbf{F}_{q_0}$, and let $\sigma' \in \mathrm{Gal}(k'/k)$ and $\sigma'' \in \mathrm{Gal}(k''/k)$ denote, respectively, the Frobenius automorphisms of k' and k'' over k. Both σ' and σ'' are given by the assignment $x \mapsto x^{q_0}$, and thus it is clear that σ' is no more than the restriction of σ''. Moreover, since P is unramified in M, the decomposition groups $D_{P''} \subseteq \mathrm{Gal}(M/F)$ and $D_{P'} \subseteq \mathrm{Gal}(K/F)$ are, respectively, isomorphic to $\mathrm{Gal}(k''/k)$ and $\mathrm{Gal}(k'/k)$. Since by construction $\varphi_{P''/P} \in \mathrm{Gal}(M/F)$ and $\varphi_{P'/P} \in \mathrm{Gal}(K/F)$ are the preimages of σ' and σ'' under these isomorphisms, we see also that $\varphi_{P'/P}$ is the restriction of $\varphi_{P''/P}$. The same then holds for the associated conjugacy classes, and hence (i) holds.

(ii) Let

$$\begin{aligned} \gamma : \mathrm{Gal}(KK'/F) &\to \mathrm{Gal}(K/F) \times \mathrm{Gal}(K'/F) \\ \sigma &\mapsto (\sigma|_K, \sigma|_{K'}) \end{aligned}$$

denote the canonical homomorphism. This is in fact an isomorphism because K and K' are assumed linearly disjoint over F. Now let $\overline{P}$ denote a prime of KK' lying above P. Then $Q = \overline{P} \cap \mathfrak{o}_K$ and $Q' = \overline{P} \cap \mathfrak{o}_{K'}$ are, respectively, primes of K and K' lying under $\overline{P}$ and over P. One checks easily that

$$\varphi_{\overline{P}/P}|_K = \varphi_{Q/P} \text{ and } \varphi_{\overline{P}/P}|_{K'} = \varphi_{Q'/P} .$$

Conversely, any pair of intermediate-level Frobenius maps must arise via γ from a conjugate of $\varphi_{\overline{P}/P}$ because γ is an isomorphism. This proves (ii).

(iii) Let the primes P, Q, and $\overline{P}$ be as shown:

$$\begin{array}{ccccc} K & \supseteq & \mathfrak{o}_K & \supseteq & \overline{P} \\ | & & | & & | \\ L & \supseteq & \mathfrak{o}_L & \supseteq & Q \\ | & & | & & | \\ F & \supseteq & \mathfrak{o}_F & \supseteq & P \end{array}$$

Again we must keep in mind two elementary, but crucial facts: the Frobenius map $\tau = \varphi_{\overline{P}/P}$ lies in the decomposition group $D_{\overline{P}} \subseteq \mathrm{Gal}(K/F)$, and

$$D_{\overline{P}} \cong \mathrm{Gal}(K_{\overline{P}}/F_P)$$

where this isomorphism is nothing more than extension of an automorphism of K over F to one of $K_{\overline{P}}$ over F_P. Now if Q is in fact a degree-one prime, which is to say that $L_Q = F_P$, then the corresponding extension of τ is ipso facto trivial on L_Q, and therefore on L. Thus $\tau \in \mathrm{Gal}(K/L)$. Conversely, if $\tau \in \mathrm{Gal}(K/L)$ and $q_0 = \mathrm{Card}(\mathfrak{o}_F/P)$, then it follows that $\alpha^{q_0} \equiv \alpha \pmod{Q}$ for $\alpha \in \mathfrak{o}_L$, from which we deduce at once that the residue fields of L and F are identical. Accordingly $L_Q = F_P$, as required. This proves the first statement of (iii).

To conclude, we establish the formula. We know now that the number of primes $\overline{P}$ of K dividing P such that $\overline{P} \cap \mathfrak{o}_L$ is of degree one over P is exactly the number of Frobenius elements defined over P that lie in $\mathrm{Gal}(K/L)$; this is just $\mathrm{Card}((P,K/F) \cap \mathrm{Gal}(K/L))$. Now the number of such primes lying over any single given degree-one prime in L is always m/f, where f be the residual degree associated with $\overline{P}$. (Clearly f is the same whether computed with respect to L or F and is therefore independent of $\overline{P} \cap \mathfrak{o}_L$, provided that this intermediate prime is indeed of degree one.) Thus the number of degree-one primes in L is f/m times the cardinality of $(P,K/F) \cap \mathrm{Gal}(K/L)$. But every element of this intersection is represented exactly f times in the form $\sigma\varphi_{\overline{P}/P}\sigma^{-1} = \varphi_{\sigma\overline{P}/P}$ as σ runs over $\mathrm{Gal}(K/F)$, and from this the formula follows at once. ❑

Arbitrary Unramified Extensions

Recall that an extension E/F is called unramified at a place u of F if there exists a chain

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E = \bigcup E_i$$

of finite extensions such that each E_i/E_{i-1} is unramified (in particular, finite and separable) at every place of E_{i-1} lying above u.

DEFINITION. Let F be a global field and P a prime in F. Then $F^{ur}(P)$ denotes the maximal subextension of $\overline{F}/F$ that is unramified at P. This is called the *maximal unramified extension* of F at P.

It is easy to check that $F^{ur}(P)$ exists (see Exercise 1 below) and is a Galois extension of F. For we have seen that each step in the tower that defines an unramified extension is the splitting field of a polynomial of the form x^r-1, and hence is itself Galois over F. Clearly,

$$\mathrm{Gal}(F^{ur}(P)/F) = \varprojlim K/F$$

where K runs over finite Galois extensions of F contained in $F^{ur}(P)$. The previous proposition shows that the Frobenius classes $\varphi_{K/F}=(P,K/F)$ patch nicely to give a class $(P,F^{ur}(P)/F)$ in $\mathrm{Gal}(F^{ur}(P)/F)$.

It is perhaps disappointing that we cannot define the Frobenius class in the absolute Galois group $\mathrm{Gal}(\overline{F}/F)$, but we point out without proof that if

$$\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\mathbf{Q}_l)$$

is a continuous representation arising from the l-adic cohomology of a smooth projective variety over F (with l a prime different from the characteristic of F), then ρ is unramified at all P outside a finite set S of primes. In other words, ρ factors through $G_{F,S}$, the Galois group of the maximal extension of F in $\overline{F}$ that is unramified outside S. Since $\mathrm{Gal}(F^{ur}(P)/F)$ maps onto $G_{F,S}$, we see that $\rho(\varphi_P)$ is well-defined at every $P \notin S$.

6.2 The Tchebotarev Density Theorem

Given a finite Galois extension K/F of global fields, we have seen how to define a map

$$\varphi = \varphi_{K/F} : \Sigma_F - S_{K/F} \to \mathrm{Gal}(K/F)^{\#}$$
$$P \mapsto \varphi_P$$

where Σ_F denotes the set of places of F, $S_{K/F}$ denotes the (finite) union of the Archimedean places and the finite places that ramify in K, and $\mathrm{Gal}(K/F)^{\#}$ is the space of conjugacy classes of $\mathrm{Gal}(K/F)$. A natural question to ask is whether every conjugacy class is φ_P for some P. The answer is *yes*, as affirmed by the following beautiful result, given here without proof.

6-3 THEOREM. (Tchebotarev) *Let $G = \mathrm{Gal}(K/F)$. Then for every conjugacy class C in G there exist infinitely many primes P such that $\varphi_P = C$. More precisely,*

$$\lim_{x\to\infty} \frac{\mathrm{Card}\{P : N(P) \le x, \varphi_P = C\}}{\mathrm{Card}\{P : N(P) \le x\}} = \frac{\mathrm{Card}(C)}{\mathrm{Card}(G)} .$$

Here, $N(P)$, the *(absolute) norm* of the prime P, is the cardinality of the associated residue field. The limit on the left side of the equality is called the *natural density* of the set described in the numerator. (As noted above, we prove a reformulation of this theorem in terms of Dirichlet density in the exercises for Chapter 7.)

An illuminating special case of this theorem arises when $F = \mathbf{Q}$ and $K = \mathbf{Q}(\zeta_m)$, the field of mth roots of unity over $\mathbf{Q}$, for some $m > 1$. Then one knows that the Galois group G of K/F is abelian, and in fact isomorphic to $(\mathbf{Z}/m\mathbf{Z})^\times$. Explicitly, each a relatively prime to m gives rise to an element

$$\sigma_a : \zeta_m \mapsto \zeta_m^a$$

of G. For every prime p not dividing m, this extension is unramified (proved for m prime in Section 4.3). Now let C be a conjugacy class in G, so that in the present case C corresponds to a singleton subset $\{a\} \subseteq (\mathbf{Z}/m\mathbf{Z})^\times$. Then one can deduce that

$$\varphi_p = \{\sigma_a\} \Leftrightarrow p \equiv a \pmod{m} .$$

Thus Tchebotarev's theorem becomes the well-known theorem of Dirichlet on primes in arithmetic progressions, namely that there are infinitely many primes p congruent to a modulo m, and, more specifically, that the density of such primes is $1/\varphi(m)$.

6.3 The Transfer Map

In preparation for the statement of the Artin reciprocity law, we now introduce a subtle and entirely group-theoretic construction that is of interest in its own right. The subtlety lies in that in general there is no homomorphism from a group to a subgroup.

Let G be any group, with H a subgroup of finite index. Let (G, G) denote the commutator subgroup; i.e., the subgroup generated by the products $sts^{-1}t^{-1}$ where s and t vary over G. Since conjugation by any element is an automorphism of G, the commutator subgroup is normal in G, and the corresponding quotient group $G^{\mathrm{ab}} = G/(G, G)$ is called the *abelianization* of G. The homomor-

phism in question is the *transfer map*, also called *die Verlagerung* by German aficionados,

$$V: G^{\text{ab}} \to H^{\text{ab}}$$

and is defined as follows.

First choose a section $s: H\backslash G \to G$; that is, a set of representatives for $H\backslash G$, the set of right cosets of H in G. Put

$$h_{x,\bar{y}} = s(\bar{y})xs(\bar{y}x)^{-1} \in H$$

where $\bar{y}x$ denotes the effect of right translation on a coset $\bar{y}$ in $H\backslash G$. (Of course, $H\backslash G$ is a G-set!) Clearly, $h_{x,\bar{y}}$ measures the failure of $s(\bar{y})x$ to equal $s(\bar{y}x)$; that is, the failure of s to be a G-map. Next define

$$\widetilde{V}(x) = \prod_{\bar{y} \in H\backslash G} h_{x,\bar{y}} \mod (H, H) .$$

Thus the right-hand side is the natural image of the given product in H^{ab}.

6-4 Proposition. *The map $\widetilde{V}: G \to H^{\text{ab}}$ is a group homomorphism independent of the choice of the section $s: G \to H\backslash G$.*

Proof. First we show that $\widetilde{V}$ is independent of the choice of section. Let s' be another section. Then there is a function $\eta: H\backslash G \to H$ such that

$$s'(\bar{y}) = \eta(\bar{y})s(\bar{y})$$

for each $\bar{y} \in H\backslash G$. Given $x \in G$, the direct calculation

$$\begin{aligned}\prod_{\bar{y}} s'(\bar{y})xs'(\bar{y}x)^{-1} &= \prod_{\bar{y}} \eta(\bar{y})s(\bar{y})x[\eta(\bar{y})s(\bar{y}x)]^{-1} \\ &= \prod_{\bar{y}} \eta(\bar{y})s(\bar{y})xs(\bar{y}x)^{-1}\eta(\bar{y})^{-1}\end{aligned}$$

shows that we may calculate $\widetilde{V}(x)$ using either section and obtain the same results modulo the commutator subgroup (H, H).

We may make a similar calculation to see that $\widetilde{V}$ is a group homomorphism:

$$\begin{aligned}\tilde{V}(x_1x_2) &= \prod_{\bar{y}} s(\bar{y})x_1x_2s(\bar{y}x_1x_2)^{-1} \mod(H,H)\\ &= \prod_{\bar{y}} s(\bar{y})x_1s(\bar{y}x_1)^{-1}\cdot s(\bar{y}x_1)x_2s(\bar{y}x_1x_2)^{-1} \mod(H,H)\\ &= \prod_{\bar{y}} s(\bar{y})x_1s(\bar{y}x_1)^{-1}\cdot \prod_{\bar{y}} s(\bar{y}x_1)x_2s(\bar{y}x_1x_2)^{-1} \mod(H,H)\\ &= \tilde{V}(x_1)\tilde{V}(x_2)\ .\end{aligned}$$

In moving from the second line to the third, we note that the indicated trios of factors all lie in H, whence all of the right hand-trios can be accumulated modulo (H,H) into a single product. In moving from the third to the fourth, we note that as $\bar{y}$ varies over $H\backslash G$, so does $\bar{y}x_1$. ❑

In consequence of this proposition, it follows from the universal property of the abelianization of a group that $\tilde{V}$ induces a unique map

$$V\colon G^{\mathrm{ab}}\to H^{\mathrm{ab}}$$

which we call the *transfer map*. We also write $V_{G,H}$ for this map to emphasize the domain and codomain. From the previous proposition it follows that the transfer map is completely intrinsic to G and H, and independent of the choice of section. Moreover, it satisfies a kind of transitivity:

6-5 PROPOSITION. (Transitivity of the Transfer Map) *If $H\subseteq K\subseteq G$, then*

$$V_{G,H} = V_{K,H}\circ V_{G,K}\ .$$

PROOF. Exercise. ❑

In his book *The Theory of Groups*, M. Hall gives an alternative development of the transfer map via *monomial representations* (1959, pp. 201–203).

6.4 Artin's Reciprocity Law

One of the major success stories in number theory this century has been the work of Takagi and Artin on the description of abelian extensions of global fields. This is codified elegantly and concisely by the Artin reciprocity law. In this section we shall, without proof, state this law simultaneously for global and local fields and indicate its associated functorial properties. We begin with a few preliminary considerations.

Let F be a global or local field. Put

$$C_F = \begin{cases} F^* & \text{if } F \text{ is local}\\ \mathbf{I}_F/F^* & \text{if } F \text{ is global}.\end{cases}$$

We know that this is a locally compact abelian group. Moreover, if K/F is a finite extension, we will be concerned with two natural homomorphisms:

$$j_{K/F} : C_F \to C_K \quad \text{and} \quad N_{K/F} : C_K \to C_F \ .$$

The first map is simply that induced by inclusion. The second is the norm homomorphism, which in the global case is induced by

$$(x_v)_v \mapsto (\prod_{v|u} N_v(x_v))_u$$

where $N_v : K_v \to F_u$ is the ordinary norm. Observe that this idele class version of the norm is well-defined: the ordinary version maps integers to integers (cf. Appendix B, Section 2), and Proposition 4-39 shows that elements of K map to elements of F. Note also that according to Exercise 3 below, the image of $N_{K/F}$ is an open subgroup of C_F.

Next fix a separable algebraic closure $\overline{F}$ and put

$$\Gamma_K = \mathrm{Gal}(\overline{F}/K)$$

for any extension K/F with $K \subseteq \overline{F}$. To describe the functoriality of Artin reciprocity, we shall also need two maps on the Galois side. The first is simply the inclusion

$$i_{K/F} : \Gamma_K \to \Gamma_F \ .$$

The second, which goes in the opposite direction, is the more subtle transfer map

$$V : \Gamma_F^{\mathrm{ab}} \to \Gamma_K^{\mathrm{ab}}$$

defined as above on the abelianizations of the domain and codomain.

Before stating Artin's reciprocity law, let us take note of the relationship between the cokernel of the norm map and the Galois group for four particular extensions K/F.

CASE 1. Let $F = \mathbf{R}$ and $K = \mathbf{C}$. Then $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \{1, \rho\}$, where ρ denotes complex conjugation. Moreover, the cokernel of the norm map

$$N_{\mathbf{C}/\mathbf{R}} : \mathbf{C}^* \to \mathbf{R}^*$$

is simply the quotient of $\mathbf{R}^*$ by the nonzero squares, which is to say the cyclic group of order 2. Hence there is a unique abstract isomorphism between $\mathbf{R}^*/N(\mathbf{C}^*)$ and $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ sending the class of -1 to ρ.

CASE 2. Let $F = \mathbf{C}$. Then since the complex numbers are algebraically closed, K must also equal $\mathbf{C}$, and both the cokernel of the norm map and the Galois group are trivial.

CASE 3. Let p be an odd prime, and let $F = \mathbf{Q}_p$ and $K = \mathbf{Q}_p(\delta)$, where $\delta^2 = 2$. Then

$$N_{K/F}(K^*) = \{r \in \mathbf{Q}_p^* : r = x^2 - 2y^2, \text{ for some } x, y \in \mathbf{Q}_p\}\ .$$

It is a good exercise to check that this norm subgroup has index 2 in $\mathbf{Q}_p^*$. Of course, $\mathrm{Gal}(K/F)$ is also cyclic of order 2.

CASE 4. Let $F = \mathbf{F}_q$, and let K be any finite extension. Note that the norm map from K^* to $\mathbf{F}_q^*$ is always surjective, and hence has trivial cokernel. Hence the situation here is very different from that of a local or global field.

6-6 THEOREM. (Artin Reciprocity) *Let F be a global field or a local field. Then there exists a homomorphism, called the* Artin map,

$$\theta_F : C_F \to \mathrm{Gal}(\overline{F}/F)^{\mathrm{ab}} = \Gamma_F^{\mathrm{ab}}$$

satisfying each of the following two groups of assertions:

PART ONE—The Artin Map for Abelian Extensions

(i) *For every finite abelian extension K/F, let $\theta_{K/F}$ denote the composition of θ_F with the natural projection $\Gamma_F^{\mathrm{ab}} \to \mathrm{Gal}(K/F)$. Then $\theta_{K/F}$ is surjective with kernel $N_{K/F}(C_K)$.*

(ii) *Conversely, given any open subgroup N of C_F of finite index, there exists a finite abelian extension K/F such that $N = \mathrm{Ker}(\theta_{K/F})$. In particular,*

$$C_F/N \cong \mathrm{Gal}(K/F)\ .$$

(iii) *Let K/F be a finite abelian and unramified extension of the non-Archimedean local field F with residual extension k'/k. Then we have explicitly*

$$\theta_{K/F}(x) = \varphi^{v(x)}$$

where φ is the Frobenius element of $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(k'/k) = \langle \varphi \rangle$.

(iv) *Let K/F be a finite abelian extension of global fields, and let P be a finite prime in F that is unramified in K. Denote by x_P the class in C_F defined by the idele*

$$\widetilde{x}_P = (1,\ldots,1,\underset{\substack{\uparrow \\ \text{place } P}}{\pi},1,\ldots,1)$$

all of whose components are 1 *except at the place defined by P, where the component is a uniformizing parameter π. Then we have*

$$\theta_{K/F}(x_p) = \varphi_P$$

where $\varphi_P=(P,K/F)$. [Note that since K/F is abelian, the Frobenius conjugacy class φ_P is in fact a single element of $\mathrm{Gal}(K/F)$.]

PART TWO—Functoriality

Let K/F be a finite separable extension, not necessarily abelian (with F either global or local). Then we have the following two commutative diagrams:

(i)

$$\begin{array}{ccc} C_K & \xrightarrow{\theta_K} & \Gamma_K^{\mathrm{ab}} \\ N_{K/F}\downarrow & & \downarrow i_{K/F} \\ C_F & \xrightarrow[\theta_F]{} & \Gamma_F^{\mathrm{ab}} \end{array}$$

(ii)

$$\begin{array}{ccc} C_K & \xrightarrow{\theta_K} & \Gamma_K^{\mathrm{ab}} \\ j_{K/F}\uparrow & & \uparrow V \\ C_F & \xrightarrow[\theta_F]{} & \Gamma_F^{\mathrm{ab}} \end{array}$$

Moreover, if K_1/F is an abelian extension with subextension K/F, then we have a further commutative diagram

(iii)

$$\begin{array}{ccc} F^*/N_{K_1/F}(K_1^*) & \xrightarrow{\theta_{K_1/F}} & \mathrm{Gal}(K_1/F) \\ \text{proj} \downarrow & & \downarrow \text{proj} \\ F^*/N_{K/F}(K^*) & \xrightarrow[\theta_{K/F}]{} & \mathrm{Gal}(K/F) \end{array}$$

Note well that the inclusion-induced map on the class group side corresponds to the transfer map on the Galois side and that the inclusion map on the Galois side corresponds to the norm map on the class group side. In the abelian case, we may simply identify the projections.

6.5 Abelian Extensions of $\mathbf{Q}$ and $\mathbf{Q}_p$

In this section, working over either $\mathbf{Q}$ or $\mathbf{Q}_p$, we consider class field theory in a particular and concrete setting. We prepare with some general field-theoretic notions.

Let F be a field, for which we implicitly fix an algebraic closure. If K_1 and K_2 are Galois extensions of F, then so is their compositum K_1K_2, and in fact we have an embedding

$$\begin{aligned} \mathrm{Gal}(K_1K_2/F) &\to \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F) \\ \sigma &\mapsto (\sigma|_{K_1}, \sigma|_{K_2}) \end{aligned}$$

which is an isomorphism if K_1 and K_2 have intersection F. Thus if K_1 and K_2 are moreover abelian extensions, so again is their compositum. Thus there exists a maximal abelian extension F^{ab} of F, which is precisely the compositum of all abelian extensions of F within its algebraic closure.

Henceforth, for any $n \geq 1$, F_n denotes the field obtained by adjoining the nth roots of unity to F (again, within its fixed algebraic closure). We shall soon see that this is always a finite Galois extension of F. We further let F_∞ denote the compositum of all of the F_n, $n \geq 1$.

We now state the main theorems of this section.

6-7 THEOREM. *Let F be a local or global field. Then for all n, F_n is a finite abelian extension. Moreover, the following assertions hold:*

(i) *If $F = \mathbf{Q}$, then $\mathrm{Gal}(F_n/F) \cong (\mathbf{Z}/n\mathbf{Z})^\times$ by an isomorphism that associates $a \in (\mathbf{Z}/n\mathbf{Z})^\times$ with the automorphism of F_n induced by $\omega \mapsto \omega^a$, where ω is a primitive nth root of unity. Consequently, $F_\infty \subseteq F^{\mathrm{ab}}$.*

(ii) *If $F=\mathbf{Q}_p$ and n is relatively prime to p, then F_n/F is unramified, with* $\mathrm{Gal}(F_n/F)$ *cyclic. In fact, every finite unramified extension of $\mathbf{Q}_p$ occurs as some F_n, with $(p,n)=1$.*

(iii) *If $F=\mathbf{Q}_p$ and n is a power of p, then F_n/F is totally ramified, with* $\mathrm{Gal}(F_n/F)\cong(\mathbf{Z}/n\mathbf{Z})^\times$.

6-8 THEOREM. (Kronecker-Weber) *Let F be either* $\mathbf{Q}$ or $\mathbf{Q}_p$. *Then $F_\infty=F^{\mathrm{ab}}$.*

REMARK. Let $F=\mathbf{Q}$. Then by the Kronecker-Weber theorem, given any finite abelian extension K of F, we can find a positive integer n such that K is contained in the field $F_n=\mathbf{Q}(e^{2\pi i/n})$. Thus one can think of K as being generated by the values of the function $e^{2\pi iz}$ at rational arguments. Kronecker's *Jugendtraum* (youthful dream) was to hope that any finite abelian extension of a number field F could be generated by values at algebraic arguments of a suitably chosen set of transcendental functions. This dream is realized for imaginary quadratic fields F, where the abelian extensions are all generated by the values of elliptic functions at "division points." Further progress has been made by Shimura and others. Kronecker's dream has in fact influenced much of modern number theory.

PROOF OF THEOREM 6-7. We begin with some basic Galois theory. Let F be any field with separable algebraic closure $\bar{F}$. For positive n, consider the equation

$$f(x)=x^n-1$$

over F. Then its splitting field is precisely F_n. If $\mathrm{char}(F)=p>0$, then there are no nontrivial p-power roots of unity in $\bar{F}$. Thus if we write $n=p^rm$, with m prime to p, the nth roots of unity in $\bar{F}$ are the same as the mth roots of unity. Therefore, in the case of positive characteristic p, we can and shall assume that n is prime to p.

Let ω be a primitive nth root of unity in $\bar{F}$, so that $\omega^n=1$, but $\omega^m\neq 1$ for any positive m smaller than n. Indeed, such an ω must exist because the formal derivative of f

$$f'(x)=nx^{n-1}$$

is nonzero for nonzero x—after all, n is assumed prime to p in positive characteristic—and therefore f must have n distinct roots in $\bar{F}$. Hence this necessarily cyclic group of solutions must have order n and, of course, a generator ω. From this we see at once that $F_n=F(\omega)$ and that F_n is the splitting field of a separable polynomial over F. Accordingly, F_n is a finite Galois extension of F.

Fix a primitive nth root of unity ω. Then ω^r is again a primitive nth root of unity if and only if r is an integer prime to n. In this way we obtain exactly

$\varphi(n)$ primitive roots. Now if $\sigma \in G = \mathrm{Gal}(F_n/F)$, it must send ω to another primitive nth root of unity. Thus we must have

$$\sigma(\omega) = \omega^{a_\sigma}$$

for some $a_\sigma \in (\mathbf{Z}/n\mathbf{Z})^\times$. Moreover, for $\sigma, \tau \in G$,

$$\omega^{a_{\sigma\tau}} = (\sigma\tau)(\omega) = \sigma(\omega^{a_\tau}) = \omega^{a_\sigma a_\tau} \ .$$

Thus $a_{\sigma\tau} = a_\sigma a_\tau$, and so we have a homomorphism of groups

$$\gamma: G \to (\mathbf{Z}/n\mathbf{Z})^\times \ .$$

Since σ is the identity of G if and only if ω^{a_σ} is ω itself, which is to say, if and only if $a_\sigma = 1$ in $(\mathbf{Z}/n\mathbf{Z})^\times$, it follows that γ is injective and that G is abelian.

Keeping in mind that ω generates F_n over F, each element $a \in (\mathbf{Z}/n\mathbf{Z})^\times$ conversely gives rise to an automorphism σ_a of F_n defined by

$$\sigma_a(\omega) = \omega^a \ .$$

However, this might not be an element of G by virtue of its failure to restrict to the identity on F, and this will indeed occur if some power of ω lying in F is moved by σ_a. Hence in general γ is not surjective.

Before specializing to $\mathbf{Q}$ or $\mathbf{Q}_p$, we observe that for any $d|n$, we may define a factor $f_d(x)$ of $f(x)$ by setting

$$f_d(x) = \prod_{b \in (\mathbf{Z}/d\mathbf{Z})^\times} (x - \omega^{bn/d}) \ .$$

Then clearly,

$$f(x) = \prod_{d|n} f_d(x)$$

with $f_1(x) = (x-1)$. We customarily call f_n the nth *cyclotomic polynomial*. Since

$$f_n(x) = \frac{x^n - 1}{\prod_{d|n, d \neq n} f_d(x)}$$

we see inductively that each cyclotomic polynomial lies in $F[x]$. Moreover, since each is monic, it follows from the Euclidean algorithm that its coefficients in fact lie in the subring of F generated by 1. In this sense, the cyclotomic poly-

nomials are generic over any field, although they may or may not be irreducible depending upon F.

With these preliminaries in hand, let us now proceed to each of the three statements of the first theorem.

(i) Now let $F=\mathbf{Q}$. Then for $n\geq 3$, F contains no nth root of unity, and therefore ω^a does not lie in F for any a prime to n. Moreover, F_n is simply the splitting field of the cyclotomic polynomial f_n, and elements of G permute the primitive roots of unity. Thus to show that γ is an isomorphism, it suffices to show that $f_n(x)$ is irreducible, for then the order of G will be the degree of f_n, which is clearly $\varphi(n)$, the order of $(\mathbf{Z}/n\mathbf{Z})^\times$.

Let $g(x)$ be the irreducible factor of $f_n(x)$ that is the minimal polynomial of ω over F. Since g is the product of linear factors of the form $(x-\omega^a)$, its coefficients are both rational and integral over $\mathbf{Q}$, which is to say that $g(x)\in\mathbf{Z}[x]$. We claim that it is enough to show that for every prime p not dividing n, ω^p is also a root of g. For this implies by iteration that ω^a is a root of g for all a prime to n, thus forcing $g=f_n$. Write

$$f_n(x) = g(x)h(x)$$

with h necessarily having integral coefficients because g is monic. If $g(\omega^p)$ is not zero, then $h(\omega^p)$ must be, and therefore ω is a root of $h(x^p)$, which is congruent to $h(x)^p$ modulo p. So, g and h have a common root when reduced modulo p, contradicting the separability of f_n modulo p that obtains whenever p does not divide n. This contradiction shows that ω^p is indeed a root of g, as claimed.

To summarize, we have the isomorphism

$$\gamma: G \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^\times$$
$$\sigma \mapsto a_\sigma$$

in the case $F=\mathbf{Q}$.

(ii) In the case that $F=\mathbf{Q}_p$, we know by Proposition 4-25 that a finite extension of F is unramified if and only if it is of the form F_n, with n relatively prime to p. Such extensions are moreover cyclic by Lemma 4-24.

(iii) Finally, we assume that $F=\mathbf{Q}_p$ and that $n=p^r$. We still have the injective homomorphism from $G=\mathrm{Gal}(F_n/F)$ into $(\mathbf{Z}/n\mathbf{Z})^\times$ that we constructed previously. As in part (i), to show that this map is moreover an isomorphism, it suffices to show that the order of G is again $\varphi(n)$.

Let ω be a primitive nth root of unity in F_n, so that in fact $F_n=F(\omega)$, and set

$$\zeta = \omega^{p^{r-1}} .$$

Then ζ is a primitive pth root of unity. Now define

$$f(x) = \sum_{j=0}^{p-1} x^{jp^{r-1}} .$$

Note that $f(x)$ is irreducible because $g(x)=f(x+1)$ is an Eisenstein polynomial. [That is, the leading coefficient of $g(x)$ does not lie in the unique prime ideal of $\mathbf{Z}_p$, but all of the other coefficients do, and the constant term does not lie in the square of this ideal.] It follows that

$$f(\omega) = \sum_{j=1}^{p-1} \omega^{jp^{r-1}} = \sum_{j=1}^{p-1} \zeta^j = 0$$

whence f is the irreducible polynomial of ω over F. But of course

$$\deg f = (p-1)p^{r-1} = \varphi(n)$$

showing that the degree of the extension F_n/F, and hence the order of G, is precisely $\varphi(n)$, as required.

It remains only to show that F_n/F is totally ramified. To begin, let $\pi=\omega-1$, so that π is a root of the irreducible polynomial $g(x)$, which, too, has degree $\varphi(n)$ over F. Then $F_n=F(\pi)\cong F[x]/(g(x))$. The residual extension $\mathbf{F}_{(n)}$ is still generated over $\mathbf{F}_p$ by the image $\bar{x}$ of x. But happily

$$\bar{g}(x) = x^{\varphi(n)}$$

where $\bar{g}(x)$ is the reduction of $g(x)$ modulo p, whence $\bar{x}=0$. (Eisenstein!) This implies that $\mathbf{F}_{(n)}=\mathbf{F}_p$, showing that F_n/F is totally ramified, as required. ❑

Proof of the Kronecker-Weber Theorem: The Local Case

We first consider the local situation, so that $F=\mathbf{Q}_p$. By the previous theorem, we have the following inclusions:

$$\mathbf{Q}_p = F \subseteq F^{\mathrm{ur}} = \bigcup_{(p,n)=1} F_n \subseteq F_\infty \subseteq F^{\mathrm{ab}}$$

where F_n, F_∞, and F^{ab} are as above, and F^{ur} is the maximal unramified extension of F in the given algebraic closure.

Recall that according to our statement of Artin reciprocity, for every finite abelian extension K/F there is a canonical isomorphism between $\text{Gal}(K/F)$ and $F^*/N_{K/F}(K^*)$. Moreover, every open subgroup of F^* is a norm subgroup; that is, is of the form $N_{K/F}(K^*)$ for some finite abelian extension K of F. Consequently, since F^{ab} is the compositum (and hence direct limit) of such extensions K, we can identify

$$\text{Gal}(F^{\text{ab}}/F) \cong \varprojlim_K \text{Gal}(K/F)$$

with the projective completion of F^*; that is,

$$\text{Gal}(F^{\text{ab}}/F) \cong \varprojlim_N F^*/N$$

where the limit is taken over open subgroups N of F^*. Next recall that we have a short exact sequence

$$1 \to \mathfrak{o}_F^\times \to F^* \xrightarrow{v_F} \mathbf{Z} \to 0 \tag{6.1}$$

which splits once we choose a uniformizing parameter π, via $\psi:\mathbf{Z} \to F^*$, $\psi(n) = \pi^n$. For every open subgroup N of F^*, this yields another split short exact sequence

$$1 \to \mathfrak{o}_F^\times / \mathfrak{o}_F^\times \cap N \to F^*/N \xrightarrow{\bar{v}_F} \mathbf{Z}/n\mathbf{Z} \to 0 \ .$$

With the existence of a left inverse for $\bar{v}_F$ in hand, we can take the corresponding profinite limits to obtain

$$1 \to \mathfrak{o}_F^\times \to \text{Gal}(F^{\text{ab}}/F) \xrightarrow{\varphi} \hat{\mathbf{Z}} \to 0 \tag{6.2}$$

which defines a projection φ from $\text{Gal}(F^{\text{ab}}/F)$ onto $\hat{\mathbf{Z}}$. (From the proof of Theorem 1-14, we know that a profinite group is the projective limit of its quotients by open normal subgroups. Since the subgroups $\mathfrak{o}_F^\times \cap N$ are cofinal among the open subgroups of $\mathfrak{o}_F^\times$, the projective limit of the corresponding quotients is precisely $\mathfrak{o}_F^\times$ itself.) And we have a final short exact sequence

$$1 \to \text{Gal}(F^{\text{ab}}/F^{\text{ur}}) \to \text{Gal}(F^{\text{ab}}/F) \xrightarrow{\rho} \hat{\mathbf{Z}} \to 0 \tag{6.3}$$

derived from the projection ρ from Gal(F^{ab}/F) onto Gal(F^{ur}/F) via the natural identification of Gal(F^{ur}/F) with $\text{Gal}(\overline{\mathbf{F}}/\mathbf{F}) \cong \hat{\mathbf{Z}}$, where $\mathbf{F}=\mathbf{F}_p$ is the residue field of F.

6-9 LEMMA. *The projection φ defined in sequence 6.2 may be identified with the natural projection ρ of* Gal(F^{ab}/F) *onto* Gal(F^{ur}/F). *Consequently we have an isomorphism* $\text{Gal}(F^{ab}/F^{ur}) \cong \mathfrak{o}_F^\times$.

To prove the main statement, we must produce a compatible family of homomorphisms from

> the quotients $\bar{v}_F(F^*/N)$, N open, that appear as factors of the projective limit that constitutes the cokernel in sequence 6.2

to

> the groups Gal(K/F), K unramified, that appear as factors of the projective limit that constitutes the cokernel in sequence 6.3

such that the induced map on the respective projective limits is an isomorphism α satisfying $\rho = \alpha \circ \varphi$. The following lemma contains the technical key:

6-10 LEMMA. *Let K be a finite abelian extension of F with ring of integers $\mathfrak{o}_K$. Then the following statements are equivalent:*

(i) *The extension K/F is unramified.*

(ii) $N_{K/F}(\mathfrak{o}_K^\times) = \mathfrak{o}_F^\times$.

Moreover, in this case $F^*/N_{K/F}(K^*)$ is a quotient of $v_F(F^*)$.

PROOF. Let $\mathbf{F}'/\mathbf{F}$ be the residual extension corresponding to K/F, and as usual, put $f=[\mathbf{F}':\mathbf{F}]$ and $n=[K:F]=ef$, where e is the ramification index. Let π_F and π_K denote, respectively, the uniformizing parameters for $\mathfrak{o}_F$ and $\mathfrak{o}_K$. Then from sequence 6.1 we get

$$F^* = \mathfrak{o}_F^\times \times \mathbf{Z} \quad \text{and} \quad K^* = \mathfrak{o}_K^\times \times \mathbf{Z}$$

and this is compatible with the group action from Gal(K/F). Recalling that the norm of π_K is π_F^f, one then easily obtains

$$F^*/N_{K/F}(K^*) \cong \mathfrak{o}_F^\times / N_{K/F}(\mathfrak{o}_K^\times) \times (\mathbf{Z}/f\mathbf{Z})\,.$$

Since $F^*/N_{K/F}(K^*)$ is isomorphic to Gal(K/F), its order is n. Thus K/F is unramified if and only if $n=f$, which is to say, if and only if $N_{K/F}(\mathfrak{o}_K^\times)=\mathfrak{o}_F^\times$. The final statement is now obvious. ❑

REMARK. We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \to & 1+\pi_K\mathfrak{o}_K & \to & \mathfrak{o}_K^\times & \to & \mathbf{F}'^* & \to & 1 \\ & & \downarrow N & & \downarrow N & & \downarrow N & & \\ 1 & \to & 1+\pi_F\mathfrak{o}_F & \to & \mathfrak{o}_F^\times & \to & \mathbf{F}^* & \to & 1 \end{array}$$

Since the norm map on the (finite) residue fields is always surjective, it follows readily that $N(\mathfrak{o}_K^\times)=\mathfrak{o}_F^\times$ if $N(1+\pi_K\mathfrak{o}_K)=1+\pi_F\mathfrak{o}_F$. Thus if the norm fails to be surjective, it already fails at this level.

PROOF OF LEMMA 6-9. Suppose that K_1 is a finite abelian extension of F and that K is any Galois subextension contained therein. From the diagram

$$\begin{array}{ccccc} F^*/N_{K_1/F}(K_1^*) = & \mathfrak{o}_F^\times/N_{K_1/F}(\mathfrak{o}_{K_1}^\times) & \times & v_F(F^*)/v_F(N_{K_1/F}(\mathfrak{o}_{K_1}^\times)) \\ \downarrow & \downarrow & & \downarrow \\ F^*/N_{K/F}(K^*) = & \mathfrak{o}_F^\times/N_{K/F}(\mathfrak{o}_K^\times) & \times & v_F(F^*)/v_F(N_{K/F}(\mathfrak{o}_K^\times)) \end{array}$$

we see that the canonical projection on the left decomposes into the direct product of the two canonical projections indicated on the right. In the case that K is the maximal unramified subextension of K_1, it follows from the previous lemma that Gal$(K/F)\cong F^*/N_{K/F}(K^*)$ is in fact isomorphic to the right-hand factor on the second line. Moreover, since K_1/K is then totally ramified, the projection on the right is the identity map, and hence we have an isomorphism

$$\alpha_{K_1}: v_F(F^*/N_{K_1/F}(K_1^*)) \xrightarrow{\cong} \text{Gal}(K/F) \quad .$$

If K_1' is another finite abelian extension of F that contains K_1 with maximum unramified subextension K'/F, we have a diagram

$$\begin{array}{ccc} \bar{v}_F(F^*/N_{K_1/F}(K_1^*)) & \xleftarrow{\text{proj}} & \bar{v}_F(F^*/N_{K_1'/F}(K_1'^*)) \\ \downarrow & & \downarrow \\ \bar{v}_F(F^*/N_{K/F}(K^*)) & \leftarrow & \bar{v}_F(F^*/N_{K'/F}(K'^*)) \\ \downarrow & & \downarrow \\ \text{Gal}(K/F) & \leftarrow & \text{Gal}(K'/F) \end{array}$$

where the vertical sequences constitute α_{K_1} and $\alpha_{K_1'}$, respectively. To show that these maps are compatible with the projective systems is to show the commutativity of this diagram, which easily reduces to the commutativity of the lower square. But if we unwind the definitions and identifications, this follows at once from the explicit description of the Artin map given for local fields in Part One, statement (iii), of the Artin reciprocity law (Theorem 6-6).

From this analysis we see that the maps α_{K_1} indeed induce an isomorphism α of projective limits

$$\alpha : \varprojlim \bar{\nu}_F(F^*/N_{K_1/F}(K_1^*)) \xrightarrow{\cong} \varprojlim \mathrm{Gal}(K/F) = \mathrm{Gal}(F^{\mathrm{ur}}/F)$$

where the limit on the left is taken over all finite abelian extensions of F and the limit on the right over all finite unramified extensions of F. In view of the remarks immediately following the statement of the lemma, it now suffices to show that α moreover satisfies the condition $\rho = \alpha \circ \varphi$, where ρ and φ are defined by sequences 6.2 and 6.3 above. This amounts to checking the commutativity of the diagram

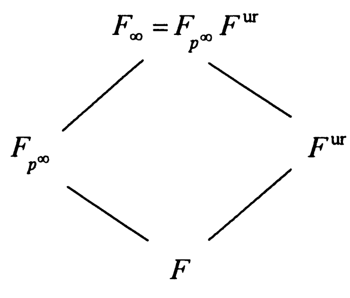
$$\begin{array}{ccc} F^*/N_{K_1/F}(K_1^*) & \to & \mathrm{Gal}(K_1/F) \\ \downarrow & & \downarrow \\ F^*/N_{K/F}(K^*) & \to & \mathrm{Gal}(K/F) \end{array}$$

where the vertical maps are the canonical projections and the horizontal maps are the isomorphisms $\theta_{K_1/F}$ and $\theta_{K/F}$. But this is no more than an element of the functoriality of the Artin map. [See Theorem 6-6, Part Two, diagram (iii).] ❑

We now return to the proof of the Kronecker-Weber theorem. By the first lemma, which holds for arbitrary local F, we have

$$\mathrm{Gal}(F^{\mathrm{ab}}/F^{\mathrm{ur}}) \cong \mathfrak{o}_F^\times .$$

(The compositum of local fields is local by Zorn's Lemma.) Now let $F = \mathbf{Q}_p$, and consider the diagram



where F_{p^∞} is the extension of F obtained by adjoining all roots of unity of order a power of p. One checks easily that F_{p^∞} and F^{ur} are linearly disjoint over F. (It suffices to verify this for finite totally ramified and unramified extensions; see Exercise 2 below.) Thus from Theorem 6-7, part (iii), we may deduce that

$$\text{Gal}(F_\infty/F^{\text{ur}}) \cong \text{Gal}(F_{p^\infty}/F) \cong \varprojlim_n (\mathbf{Z}/p^n\mathbf{Z})^\times \cong \mathbf{Z}_p^\times .$$

Accordingly, the Galois groups of both F_∞ and F^{ab} over F^{ur} are isomorphic to the p-adic units, and since $F^{\text{ur}} \subseteq F_\infty \subseteq F^{\text{ab}}$, we get an identification of F_∞ with F^{ab} once we prove the following:

6-11 LEMMA. *Any surjective (continuous) homomorphism $\mu:\mathbf{Z}_p^\times \to \mathbf{Z}_p^\times$ is an isomorphism.* ❑

The proof of this lemma is left as an exercise. (One approach is to use that $\mathbf{Z}_p^\times$ is isomorphic to $\mathbf{F}_p^* \times \mathbf{Z}_p$ and that $\mathbf{Z}_p$ is Noetherian as a module over $\hat{\mathbf{Z}}$.) Thus we have established that every abelian extension of $\mathbf{Q}_p$ is cyclotomic. ❑

Proof of the Kronecker-Weber Theorem: The Global Case

We now consider the global case $F=\mathbf{Q}$. By Artin reciprocity (Theorem 6-6), every finite abelian extension $K/\mathbf{Q}$ determines a canonical open subgroup $U=U(F)$ of $C_\mathbf{Q}=\mathbf{I}_\mathbf{Q}/\mathbf{Q}^*$ such that $C_\mathbf{Q}/U$ identifies, via the Artin map, with $\text{Gal}(K/\mathbf{Q})$. For each $m\geq 1$, let U_m denote the open subgroup associated with the mth cyclotomic extension $F_m=\mathbf{Q}(e^{2\pi i/m})$. Since the first part of the reciprocity law implies in particular that the correspondence between open subgroups and finite abelian extensions is bijective and inclusion-reversing, we need only show that U contains U_m for some m. To do this, we must first understand open subgroups of $\mathbf{I}_\mathbf{Q}$ and $\mathbf{I}_\mathbf{Q}/\mathbf{Q}^*$ somewhat better. The following result is key:

6-12 PROPOSITION. *The idele group admits a decomposition as a direct product of topological groups*

$$\mathbf{I}_\mathbf{Q} = \mathbf{Q}^* \times \mathbf{R}_+^\times \times \hat{\mathbf{Z}}^\times$$

where $\hat{\mathbf{Z}}^\times = \varprojlim_n (\mathbf{Z}/n\mathbf{Z})^\times = \prod_p \mathbf{Z}_p^\times$. *Hence* $C_\mathbf{Q} = \mathbf{R}_+^\times \times \hat{\mathbf{Z}}^\times$.

PROOF. Define a map $\xi:\mathbf{I}_\mathbf{Q} \to \mathbf{Q}^*$ by

$$\xi(x) = \text{sgn}(x_\infty)\prod_p |x_p|_p^{-1}$$

for $x=(x_\infty, x_2, x_3, \ldots, x_p, \ldots)\in\mathbf{I}_\mathbf{Q}$. If m is a nonzero rational integer with prime factorization

$$m = \pm\prod_{j=1}^{r} p_j^{\alpha_j}$$

then

$$\xi(m) = \pm\prod_{j=1}^{r} |p_j|_{p_j}^{-\alpha_j} \ .$$

But the normalized absolute value of each p_j with respect to itself is p_j^{-1}, and so in fact, $\xi(m)=m$. From this we deduce that $\xi(x)=x$ for all nonzero rational x; in other words, ξ provides a continuous group-theoretic section to the diagonal embedding $\mathbf{Q}^*\rightarrow\mathbf{I}_\mathbf{Q}$. Thus we have $\mathbf{I}_\mathbf{Q}=\mathbf{Q}^*\times\text{Ker}(\xi)$. Finally, it is obvious that

$$\text{Ker}(\xi) = \mathbf{R}_+^\times \times \prod_p \mathbf{Z}_p^\times$$

whence the assertion follows. ❑

We return to the proof that for any finite abelian extension K of $F=\mathbf{Q}$, the associated open subgroup U of $C_\mathbf{Q}$ contains U_m for some $m\geq 1$. By the proposition above, any such U can be identified with an open subgroup of $\mathbf{R}_+^\times \times \hat{\mathbf{Z}}^\times$. Since the positive reals admit no nontrivial open subgroups, U must be of the form $\mathbf{R}_+^\times \times \overline{U}$, where the latter factor is an open subgroup in $\hat{\mathbf{Z}}^\times$. But an examination of the local base for the topology of $\hat{\mathbf{Z}}^\times$ at the identity—and the Chinese remainder theorem—reveals at once that U must contain some U_m, the unique subgroup of $C_\mathbf{Q}$ corresponding to $\text{Gal}(K_m/K)$.

This completes the proof of the Kronecker-Weber theorem. ❑

The Characters of $C_\mathbf{Q}$

We conclude this section by describing all of the (continuous) characters of the idele class group of $\mathbf{Q}$.

6-13 PROPOSITION. *Every character of* $\mathbf{I}_\mathbf{Q}$ *that is trivial on* $\mathbf{Q}^*$ *is a product of the form* $\chi|\cdot|_\mathbf{A}^s$, *where* χ *is a character of finite order and* s *is a complex number.*

PROOF. Let $\omega\in\text{Hom}_{\text{cont}}(\mathbf{I}_\mathbf{Q},\mathbf{C}^*)$ with $\omega|_{\mathbf{Q}^*}=1$. We have a topological isomorphism

$$\begin{aligned} \mathbf{C}^* &\to \mathbf{R}_+^\times \times S^1 \\ z = re^{it} &\mapsto (r, e^{it}) \end{aligned}$$

which we regard as an identification. Accordingly, we can decompose ω as the product $\omega_r\omega_u$ with $\omega_r : \mathbf{I_Q} \to \mathbf{R}_+^\times$ and $\omega_u : \mathbf{I_Q} \to S^1$. By the previous proposition, we may view ω as a continuous character of $\mathbf{R}_+^\times \times \hat{\mathbf{Z}}^\times$. Since the second factor is compact and totally disconnected, its complex characters are of finite order. (See Chapter 3, Exercise 14. This is not true if, for example, we consider p-adic characters!) Thus $\omega_r|_{\hat{\mathbf{Z}}^\times} = 1$, while $\omega_u|_{\hat{\mathbf{Z}}^\times}$ must be of finite order. Now put $\chi(x) = \omega_u(\rho(x))$, where ρ is the projection of $\mathbf{I_Q}$ onto $\hat{\mathbf{Z}}^\times$. Since ω_r is trivial on both $\mathbf{Q}^*$ and $\hat{\mathbf{Z}}^\times$, it factors through the projection

$$\begin{aligned} \mathbf{I_Q} &\to \mathbf{R}_+^\times \\ x &\mapsto |x|_{\mathbf{A}} \end{aligned}$$

and so $\omega_r(x) = \beta(|x|_{\mathbf{A}})$ for a continuous homomorphism $\beta : \mathbf{R}_+^\times \to \mathbf{R}_+^\times$. Let $d\beta$ be the "differential" of β; that is, $d\beta(t) = \log\beta(e^t)$. Since this map is linear, it must be equivalent to multiplication by a real number y. Exponentiating, we get

$$\omega_r(x) = |x|_{\mathbf{A}}^y \ .$$

By a similar argument, we see that any continuous homomorphism $\gamma : \mathbf{R}_+^\times \to S^1$ must be of the form $a \mapsto a^{it}$ for some $t \in \mathbf{R}$. Putting all of this together, we get $\omega = \omega_r\omega_u$ with

$$\omega_r(x) = |x|_{\mathbf{A}}^y \quad \text{and} \quad \omega_u(x) = |x|_{\mathbf{A}}^{it}\chi(x)$$

for some $y, t \in \mathbf{R}$. Hence the assertion of the proposition holds with $s = y + it$. ❑

Remark. A character χ on $\mathbf{I_Q}$ that factors through $C_{\mathbf{Q}}$ and has finite order must accordingly be trivial on the $\mathbf{R}_+^\times$ component of the idele class group and hence is neither more nor less than a character of $\hat{\mathbf{Z}}^\times$. Moreover, χ further factors through some component $(\mathbf{Z}/n\mathbf{Z})^\times$ of $\hat{\mathbf{Z}}^\times$. This follows by continuity: for every rational prime p,

$$\chi(\hat{\mathbf{Z}}_p^\times) = \chi(\mathbf{Z}/p^{n_p}\mathbf{Z})^\times$$

for some n_p, where we have implicitly embedded the quotient into the inverse limit in the obvious way. Hence, since χ has finite image,

$$\chi(\hat{\mathbf{Z}}^{\times}) = \chi(\prod_p \hat{\mathbf{Z}}_p^{\times}) = \chi((\mathbf{Z}/p_1^{n_1}\cdots p_r^{n_r}\mathbf{Z})^{\times})$$

for some finite collection of primes p_j. Thus the idele class character χ induces a *Dirichlet character*, which is to say a character of $(\mathbf{Z}/n\mathbf{Z})^{\times}$ for some positive n. (Dirichlet characters are customarily extended to all of $\mathbf{Z}/n\mathbf{Z}$ by assigning zero to elements not invertible modulo n.) The smallest n that affords such a factorization is called the *conductor* of χ. Moreover, this association is patently reversible: given any Dirichlet character, we can certainly pull it back to a character of the group $\hat{\mathbf{Z}}^{\times}$, and hence to a unique idele class character on $\mathbf{I}_{\mathbf{Q}}$. Thus the rational idele class characters of finite order lie in a natural bijective correspondence with the Dirichlet characters.

Exercises

1. Let F be a global field and P a prime of F. Show that $F^{\text{ur}}(P)$ exists and is in fact given as the compositum of all finite, unramifed extensions of K/F in a fixed algebraic closure $\overline{F}$. [*Hint*: This is an exercise in cardinality. How many such K are there?]

2. Let F be a local field with finite extensions K and L that are, respectively, totally ramified and unramified. Show that K and L are linearly disjoint over F. [*Hint*: Choose a basis B for L over F such that (i) $B \subseteq \mathfrak{o}_L$ and (ii) B projects onto a basis of the corresponding residue fields. What happens to a linear dependence relation over $\mathfrak{o}_K$ when reduced modulo the unique prime of the compositum of K and L? Keep in mind that the residue extension corresponding to K/F is trivial. Conclude that B remains linearly independent over K and hence that K and L are linearly disjoint over F.]

3. Let F be a global field.

(a) Show, for every place u of F and for every positive integer n, that $(F_u^*)^n$ is an open subgroup of F_u^*. [*Hint*: First show that a subgroup G of F_u^* of finite index is open if and only if it is closed.]

(b) Show, for every place u of F and for every finite extension L of F_u, that the image of L^* under the norm map N_{L/F_u} is an open subgroup of F_u^*. [*Hint*: Note that if $n=[L:F_u]$, then $(F_u^*)^n$ is a subgroup of $N_{L/F_u}(L^*)$.]

(c) Let K/F be a finite extension. Show, for any place u of F, that the map

$$\prod_{v|u} K_v^* \to F_u^*$$
$$(x_v) \mapsto \prod_{v|u} N_{K_v/F_u}(x_v)$$

has open image.

(d) Let K/F be a finite extension. show that $N_{K/F}(C_E)$ is an open subgroup of C_F. [*Hint*: First analyze the map $N_{K/F}: \mathbf{I}_K \to \mathbf{I}_F$.]

4. Let F be a local field, and let $\theta_F : C_F \to \Gamma_F^{\mathrm{ab}}$ be the Artin map. Recall that C_F is just F^* in this local case.

(a) Show that $\theta_F(\mathfrak{o}_F^\times)$ lies in the *inertia group*

$$I = \mathrm{Ker}(\Gamma_F^{\mathrm{ab}} \to \mathrm{Gal}(\overline{\mathbf{F}}_q/\mathbf{F}_q))$$

where $\mathbf{F}_q$ is the residue field of F.

(b) Using Part One, statement (ii), of Theorem 6-6, show that θ_F induces an isomorphism of $\mathfrak{o}_F^\times$ with I.

(c) Show that the natural topology of $\mathfrak{o}_F^\times$ is identical to that induced by the norm subgroups.

5. Let F be a global field, and let $\theta_F : C_F \to \Gamma_F^{\mathrm{ab}}$ be the Artin map.

(a) Show that if F is a number field, then θ_F is surjective with kernel equal to the connected component of the identity of C_F.

(b) (Artin-Tate) Show that if F is a function field over a finite field $\mathbf{F}_q$, then θ_F is injective with dense image. Show, moreover, that each automorphism in the image restricts to an integral power of the Frobenius map $x \mapsto x^q$ on $\overline{\mathbf{F}}_q$.

✧ ✧ ✧ ✧ ✧ ✧ ✧ ✧ ✧

SPECIAL NOTE. It is beyond us to compose problems on class field theory and the relationship of Artin's reciprocity law to the classical power residue symbols, prime decompositions, etc., equal to the amazing ones found in *Algebraic*

Number Theory by Cassels and Fröhlich (1968, pp. 348–364). We encourage the reader to try all of these wonderful and productive exercises.

7
Tate's Thesis and Applications

It is well known that much information on rational primes is encoded in the Riemann zeta function $\zeta(s)$, which is defined by the absolutely convergent series

$$\zeta(s)=\sum_{n\geq 1}\frac{1}{n^s}$$

for complex numbers s such that $\mathrm{Re}(s)>1$. Moreover, this function admits an analytic continuation to the whole s-plane, except for a simple pole at $s=1$, and satisfies the functional equation

$$\xi(s)=\xi(1-s)$$

where

$$\xi(s)=\pi^{-s/2}\Gamma(\frac{s}{2})\zeta(s).$$

One establishes this analytic continuation and the functional equation by making use of the Mellin transform of the theta function

$$\theta(z)=\sum_{n\in\mathbf{Z}}e^{2\pi i n^2 z}$$

and the well-known identity

$$\sum_{n\in\mathbf{Z}}e^{-\pi n^2 t^2}=t^{-1}\sum_{n\in\mathbf{Z}}e^{-\pi n^2/t^2} \tag{7.1}$$

for $t>0$.

Euler was the first to study $\zeta(s)$, but only for s real. He established the Euler product expansion [in fact valid in the domain $\mathrm{Re}(s)>1$]

$$\zeta(s)=\prod_p\frac{1}{(1-p^{-s})}$$

where p runs over the rational primes. He also realized that the assertion $\zeta(s)$ approaches infinity as $s \to 1^+$ is equivalent to the infinitude of primes in **Z**. One could greatly generalize the zeta function with the introduction of the *Dirichlet series*. Given a multiplicative sequence $\{a_n\}_{n\geq 1}$, which is to say that $a_{mn}=a_m a_n$ whenever m and n are relatively prime, one can form the series

$$L(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$$

which is absolutely convergent in some right half-plane. Two very important examples are (i) $L(s)=\Sigma\chi(n)n^{-s}$, where χ is a Dirichlet character (for instance, as derived from the Legendre symbol), and (ii) $L(s)=\Sigma\chi(\mathfrak{a})(N\mathfrak{a})^{-s}$, where $\mathfrak{a}$ runs over the nonzero ideals of the ring of integers of a number field K and χ is a character of the ideal class group Cl_K. (In the latter example, when $\chi=1$, the resulting series is called the Dedekind zeta function of K.) A simultaneous generalization of these two is the L-function $L(s,\chi)$ associated with a (continuous) character χ of the idele class group C_K of any number field K. A substantial achievement of E. Hecke was to establish the analytic continuation and the functional equation of $L(s,\chi)$ for *any* idele class character χ by an enormously complicated application of generalized theta functions and the higher analogues of Eq. 7.1, which we now understand as consequences of the Poisson summation formula. One thing that Hecke's method could not describe satisfactorily was the nature of the global constant $W(\chi)$, the so-called *root number*, appearing in the functional equation of $L(s,\chi)$. Then, circa 1950, following a suggestion of his erstwhile thesis advisor E. Artin, J. Tate made use of Fourier analysis on adele groups to re-prove both the analytic continuation and the functional equation of $L(s,\chi)$. In the process, Tate also established local functional equations along with a factorization of the "abelian" root number, for which he gave an explicit formula.

The basic idea of Tate was to realize the local factors and the global L-functions of χ as the greatest common divisor of a family of zeta integrals, with a consequent generalization of Gauss sums. The key is to take a nice topological ring R such as $\mathbf{Q}_p$, $\mathbf{R}$, or $\mathbf{A}_\mathbf{Q}$, and to consider integrals of the form

$$z(\chi,\varphi) = \int \chi(x)\varphi(x)dx$$

where χ is a character of $R^\times$ and φ is a nice function on R. The functional equation reflects the Fourier duality between (χ,φ) and $(\check{\chi},\hat{\varphi})$, where $\hat{\varphi}$ is the Fourier transform of φ and $(\mu|\cdot|^s)^\vee = \overline{\mu}|\cdot|^{1-s}$ if μ is a unitary character of $R^\times$. Note that in the formally analogous case $R=\mathbf{F}_p$, χ is of order dividing $(p-1)$, and every function φ on R is a linear combination $\Sigma c_\psi \psi$, where ψ runs over the characters of the additive group of R; that is, elements of $\mathrm{Hom}(\mathbf{F}_p, \mathbf{C}^*)$. So,

as suggested above, in this case, $z(\chi, \varphi)$ becomes $\sum c_{\psi} g(\chi, \psi)$, where each $g(\chi, \psi)$ is the Gauss sum

$$\sum_{a=1}^{p-1} \chi(a) e^{2\pi i a b(\psi)/p}$$

for some integer $b(\psi)$. When R is a local field or the adele ring of a global field, the characters ψ of R are oscillatory and $z(\chi, \psi)$ will not converge. Here the zeta integrals make sense only for suitable functions φ and may have singularities; the true analogue of the Gauss sum turns out to be the epsilon factor $\varepsilon(\chi, \varphi)$ occurring in the functional equation. When R is the adele ring of a global field F, the multiplicative characters χ of interest will always be trivial on F^* and thus will define idele class characters.

In his thesis, Tate used some ad hoc spaces of functions over local and global fields. Here we will systematically use the spaces of Schwartz-Bruhat functions.

We end this chapter with applications, and, in particular, with a proof of the characterization of idele class characters χ via their local components χ_p, for p running over a set of primes of density greater than one-half.

7.1 Local ζ-Functions

Let F be a local field with absolute value $|\cdot|$ and Haar measure dx. Define

$$d^*x = c \cdot \frac{dx}{|x|}$$

for some fixed real number $c>0$, which we always normalize to $c=1$ for F Archimedean. Then d^*x is a Haar measure on F^*. When F is non-Archimedean, let $\mathfrak{o}_F$ denote its ring of integers, $P=P_F$ its maximal ideal, π_F the uniformizing parameter, and $\mathbf{F}_q$ the corresponding residue field. Recall that F^* is the direct product $U_F \times \mathcal{G}_F$, where U_F is the subgroup of F^* consisting of elements of unit absolute value and $\mathcal{G}_F$ is the valuation group; that is,

$$\mathcal{G}_F = \{y \in \mathbf{R}_+^\times : y=|x|, \text{ for some } x \in F^*\}.$$

Then $\mathcal{G}_F$ equals $\mathbf{R}_+^\times$ if F is Archimedean and $q^{\mathbf{Z}}$ otherwise. (Note that U_F is just the usual group of units in $\mathfrak{o}_F$ in the non-Archimedean case.)

Let $X(F^*)=\mathrm{Hom}_{\mathrm{cont}}(F^*, \mathbf{C}^*)$ denote the space of continuous group homomorphisms from F^* to $\mathbf{C}^*$. In this chapter, we refer to elements $\chi \in X(F^*)$ as *characters* of F^*. These have sometimes been called *quasi-characters.* Characters with codomain given as S^1 are here distinguished as *unitary characters.*

Hence unitary characters of F^* are ordinary group characters in the sense of Chapter 3. (Admittedly, the term has been overworked.) We see that every $\chi \in X(F^*)$ factors into the product

$$\chi = \mu|\cdot|^s$$

where μ is the pullback of a unitary character on $U_F \subseteq F^*$, uniquely defined by the restriction of χ, and s is a complex number. This is because the compactness of U_F forces its characters to be unitary, while the characters of $\mathcal{G}_F$ are all of the form $t \mapsto t^s$ for some $s \in \mathbf{C}$. A straightforward calculation shows that while s may not be uniquely determined by this factorization—examine the non-Archimedean case—nonetheless, Re(s), the real part of s, always is. Accordingly, we call Re(s) the *exponent* of χ.

The object of this section is to introduce the *local L-factor* $L(\chi)$ associated with an arbitrary character χ of F^* and to realize it as the greatest common divisor of some local zeta integrals.

We say that $\chi \in X(F^*)$ is *unramified* if $\chi|_{U_F}=1$. If F is non-Archimedean, set

$$L(\chi) = \begin{cases} (1-\chi(\pi_F))^{-1} & \text{if } \chi \text{ is unramified} \\ 1 & \text{otherwise.} \end{cases}$$

If $F=\mathbf{C}$, then U_F is S^1, and χ takes the form

$$\chi_{s,n} : re^{i\theta} \mapsto r^s e^{in\theta}$$

for some uniquely defined $s \in \mathbf{C}$ and $n \in \mathbf{Z}$. (Recall that the dual group of S^1 is the discrete group $\mathbf{Z}$; for arbitrary real n, the map $e^{i\theta} \mapsto e^{in\theta}$ is not continuous.) We then set

$$L(\chi_{s,n}) = \Gamma_{\mathbf{C}}\left(s+\frac{|n|}{2}\right) = (2\pi)^{-(s+\frac{|n|}{2})}\Gamma\left(s+\frac{|n|}{2}\right)$$

where $\Gamma(s)$ is the traditional Γ-function

$$\Gamma(x) = \int_0^\infty e^{-t}t^{x-1}\,dt$$

and $\Gamma_{\mathbf{C}}(s)=2(2\pi)^{-s}\Gamma(s)$. Finally, for $F=\mathbf{R}$, in which case $U_F=\{\pm 1\}$, we may write $\chi=\mu|\cdot|^s$, with both μ and s uniquely defined. Letting sgn denote the *sign character* $x \mapsto x/|x|$, we set

$$L(\chi)=\begin{cases}\Gamma_{\mathbf{R}}(s)\doteq\pi^{-s/2}\Gamma(s/2) & \text{if } \mu=1\\ \Gamma_{\mathbf{R}}(s+1) & \text{if } \mu=\text{sgn}.\end{cases}$$

Given a character χ of F^* and a complex number s, the product $\chi|\cdot|^s$ of course also defines a character, and one customarily writes $L(s,\chi)$ for $L(\chi|\cdot|^s)$. Moreover, we define the *shifted dual* of χ by

$$\chi^\vee=\chi^{-1}|\cdot|$$

so that

$$L((\chi|\cdot|^s)^\vee)=L(1-s,\chi^{-1}).$$

Fix a nontrivial *additive character* ψ of F; that is, a nontrivial element of $\hat{F}=\text{Hom}(F,S^1)$, the ordinary dual group of $\langle F,+\rangle$. One can show that if ψ' is any other additive character on F, then

$$\psi'(x)=\psi(ax)$$

for some $a\in F$. (See Exercise 1 below.) We will denote this character ψ_a. It follows from this that map $a\mapsto\psi_a$ is an isomorphism of topological groups from the additive group F to the dual group $\hat{F}$, and hence we have the following result, which we shall later extend to adele groups:

7-1 PROPOSITION. *Any local field F viewed as an additive locally compact topological group is isomorphic to its (unitary) dual. In fact, given any nontrivial character ψ of F, the mapping*

$$\begin{aligned}F&\to\hat{F}\\ a&\mapsto\psi_a\end{aligned}$$

is an isomorphism of topological groups. ❑

In a case such as this of a self-dual, locally compact abelian group, we may speak of a Haar measure dx as being *self-dual* if it is equal to its own dual measure in the sense defined by the Fourier inversion formula (Theorem 3-9).

We will say that a complex-valued function f on F (or F^*) is *smooth* if it is $\mathscr{C}^\infty$ for F Archimedean, and locally constant otherwise; that is, $f(x)=f(x_0)$ for all x sufficiently close to x_0. In the Archimedean case, a *Schwartz function* f on F is a smooth function that goes to zero rapidly at infinity; more precisely,

$$p(x)f(x)\to 0$$

as $x \to \infty$ for all polynomials $p(x)$. A *Schwartz-Bruhat function* is a Schwartz function if F is Archimedean, and a smooth function with compact support in the non-Archimedean case. We let $S(F)$ denote the space of Schwartz-Bruhat functions; this is clearly a complex vector space.

Given $f \in S(F)$ and the fixed additive character ψ, we may define the Fourier transform of f by

$$\hat{f}(y) = \int_F f(x)\psi(xy)\,dx\,.$$

Note that in this chapter it is convenient to drop the traditional conjugation of the second factor of the integrand; accordingly, this conjugation reappears in the Fourier inversion formula. While this is well-defined and in fact again lies in $S(F)$, it nonetheless depends on the choice of the pair (ψ, dx). In his thesis, Tate normalizes his measure to be self-dual relative to ψ, so that the identity

$$f(x) = \hat{\hat{f}}(-x)$$

holds. We shall avoid this normalization at least for the local non-Archimedean case.

Given $f \in S(F)$ and $\chi \in X(F^*)$, we define the associated *local zeta function*, or *local zeta integral*, to be

$$Z(f,\chi) = \int_{F^*} f(x)\chi(x)\,d^*x\,.$$

The main result of this section is the following:

7-2 THEOREM. *Let $f \in S(F)$ and $\chi = \mu|\cdot|^s$ with μ unitary of exponent $\sigma = \mathrm{Re}(s)$. Then the following statements hold:*

(i) *$Z(f,\chi)$ is absolutely convergent if σ is positive.*

(ii) *If $\sigma \in (0,1)$, there is a functional equation*

$$Z(\hat{f},\chi^\vee) = \gamma(\chi,\psi,dx)Z(f,\chi)$$

for some $\gamma(\chi,\psi,dx)$ independent of f, which in fact is meromorphic as a function of s.

(iii) *There exists a factor $\varepsilon(\chi,\psi,dx)$ that lies in $\mathbf{C}^*$ for all s and satisfies the relation*

$$\gamma(\chi,\psi,dx) = \varepsilon(\chi,\psi,dx)\frac{L(\chi^\vee)}{L(\chi)}\,.$$

According to part (i), $Z(\hat{f},\chi^\vee)$ converges for $\sigma<1$, and so part (ii) immediately yields a meromorphic continuation of $Z(f,\chi)=Z(f,\mu,s)$ to the whole s-plane, although initially this function is defined and holomorphic only for $\mathrm{Re}(s)>0$. Moreover, from parts (i) and (iii) we deduce that

$$L(\chi)Z(\hat{f},\chi^\vee)=\varepsilon(\chi,\psi,dx)L(\chi^\vee)Z(f,\chi).$$

Since the zeta factor on the left is absolutely convergent to the left of 1 and the epsilon factor on the right is a nonzero complex number, this implies that the poles of $Z(f,\chi)$ are no worse than those of $L(\chi)$, which is independent of f. We will see later that the "local L-factor" is given as $L(\chi)=Z(f_0,\chi)$ for some suitable f_0.

PROOF. (i) Since $\chi=\mu|\cdot|^s$ and μ is unitary, we need to show that

$$I(f,\sigma)=c\int_{F-\{0\}}|f(x)|\cdot|x|^{\sigma-1}\,dx<\infty\ .$$

First suppose that F is Archimedean. Then, since f is a Schwartz function, the integrand goes to zero rapidly as x approaches infinity. Also, as x approaches zero, the behavior of the integral is governed by the fact that $|x|^{\sigma-1}$ is integrable around zero for any positive σ. Thus the integral is finite, and we may pass to the second and final case.

Suppose next that F is non-Archimedean. Since f is then locally constant with compact support, it factors through a finite quotient group of the form

$$\pi_F^m\mathfrak{o}_F\,/\,\pi_F^n\mathfrak{o}_F$$

for some integers m and n. Hence by linearity and the translation invariance of the Haar measure, it suffices to check the assertion for functions f that are merely the characteristic functions of the various ideals $\pi_F^j\mathfrak{o}_F$. But from the decomposition

$$\pi_F^j\mathfrak{o}_F-\{0\}=\dot{\bigcup_{k=j}^{\infty}}\,\pi_F^k\mathfrak{o}_F^\times$$

it follows that

$$\begin{aligned}I(f,\sigma)&=c\int_{F-\{0\}}|f(x)|\cdot|x|^{\sigma-1}\,dx\\&=\int_{F^*}|f(x)|\cdot|x|^{\sigma}\,d^*x\end{aligned}$$

$$= \mathrm{Vol}(\mathfrak{o}_F^\times, d^*x) \sum_{k \geq j} q^{-k\sigma}$$

$$= \mathrm{Vol}(\mathfrak{o}_F^\times, d^*x) \frac{q^{-j\sigma}}{1-q^{-\sigma}}$$

which is finite for σ positive. This completes part (i).

(ii) Choose an auxiliary function $h \in S(F)$. Tate's key idea is first to prove the following:

7-3 LEMMA. *For all χ with exponent $\sigma \in (0,1)$, we have*

$$Z(f,\chi)Z(\hat{h},\chi^\vee) = Z(\hat{f},\chi^\vee)Z(h,\chi).$$

PROOF. Note that these zeta functions are well-defined at least for such σ by part (i). We may write

$$Z(f,\chi)Z(\hat{h},\chi^\vee) = \iint_{F^* \times F^*} f(x)\hat{h}(y)\chi(xy^{-1})|y|\, d^*x\, d^*y \ .$$

Since $d^*x d^*y$ is the product (Haar) measure on $F^* \times F^*$ and hence invariant under the translation $(x,y) \mapsto (x,xy)$, this double integral becomes

$$\iint_{F^* \times F^*} f(x)\hat{h}(xy)\chi(y^{-1})|xy|\, d^*x\, d^*y \ = \int_{F^*} \{f,h\}(y)\chi(y^{-1})|y|\, d^*y \qquad (7.2)$$

where

$$\{f,h\}(y) = \int_{F^*} f(x)\hat{h}(xy)|x|\, d^*x \ .$$

Both steps are justified by Fubini's theorem. The symbol $\{f,h\}$ in fact has a critical property:

CLAIM. $\{f,h\} = \{h,f\}$.

Indeed, since $c \cdot dx = |x| d^*x$, we have by definition of $\hat{h}$ that

$$\{f,h\}(y) = c \iint_{F \times F} f(x)h(z)\psi(xyz)\, dz\, dx$$

which by Fubini's theorem equals

$$c\int_F h(z)\hat{f}(yz)dz = \{h, f\}(y)$$

and thus the claim is established. The full lemma of course follows at once from Eq. 7.2. ❑

Let us now return to the proof of part (ii) of Theorem 7-2. Fix a function $f_0 \in S(F)$ and put

$$\gamma(\chi) = \gamma(\chi, \psi, dx) = \frac{Z(\hat{f}_0, \chi^\vee)}{Z(f_0, \chi)}.$$

Then by the preceding lemma, γ is independent of the choice of f_0, and we have

$$Z(\hat{f}, \chi^\vee) = \gamma(\chi, \psi, dx)Z(f, \chi)$$

as asserted. As noted above, since $Z(f, \chi)$ is defined for all χ with positive exponent, while $Z(\hat{f}, \chi^\vee)$ is defined for all χ with exponent less than unity, we will get the requisite meromorphic continuation of $Z(f, \chi)$ if we can show that $\gamma(\chi)$ is meromorphic everywhere. This will follow as a byproduct of the proof of the final assertion, where we will in fact compute $\gamma(\chi)$ for a suitable f_0.

(iii) We shall choose a special function (or family of functions) f for each of the three cases defined below. The computations are done for the standard measure dx (to be defined), which is self-dual for a standard choice of ψ. In Exercise 8 below we shall indicate the ensuing changes for an arbitrary pair (dx, ψ).

CASE ONE: $F=\mathbf{R}$. We take dx to be the usual Lebesgue measure and choose our standard character to be

$$\psi(x) = e^{-2\pi i x}.$$

As we have observed previously, every character $\chi \in \mathrm{Hom}_{\mathrm{cont}}(\mathbf{R}^*, \mathbf{C}^*)$ must be of the form $|\cdot|^s$ or $\mathrm{sgn}|\cdot|^s$, where sgn is the sign character. Suppose first that $\chi = |\cdot|^s$. Then take

$$f(x) = e^{-\pi x^2}$$

which is clearly in $S(\mathbf{R})$. Then

$$Z(f,\chi)=\int_{\mathbf{R}^*} e^{-\pi x^2}|x|^s\, d^*x \;=2\int_0^\infty e^{-\pi x^2}x^{s-1}dx\,.$$

Putting $u=\pi x^2$, the integral reduces to

$$Z(f,\chi)=\pi^{-s/2}\int_0^\infty e^{-u}u^{s/2-1}du=\pi^{-s/2}\Gamma(s/2)$$

since in general,

$$\Gamma(s/2)=\int_0^\infty e^{-u}u^{s/2-1}du\,.$$

Checking this against the definition of $L(\chi)$, we have shown that $Z(f,\chi)=L(\chi)$ for all characters χ of this form. Next recall that

$$\hat{f}(y)=\int_{\mathbf{R}} e^{-\pi x^2}e^{-2\pi ixy}dx=f(x)\,.$$

(This classical formula can be proven by contour integration.) Thus we have

$$Z(\hat{f},\chi^\vee)=\int_{\mathbf{R}^*} f(x)\chi^\vee(x)\,d^*x$$

which equals $L(\chi^\vee)$ by what was just shown. So for $\chi=|\cdot|^s$, we have

$$\gamma(x)=\frac{L(\chi^\vee)}{L(\chi)}$$

and we may put $\varepsilon(\chi)=\varepsilon(\chi,\psi,dx)=1$.

For F real, there still remains the possibility that $\chi=\operatorname{sgn}|\cdot|^s$. Under these circumstances take

$$f(x)=xe^{\pi x^2}\,.$$

Then since $\operatorname{sgn}(x)=x/|x|$, we find that

$$\begin{aligned} Z(f,\chi) &= \int_{\mathbf{R}^*} xe^{-\pi x^2} \cdot \frac{x}{|x|} \cdot |x|^s \, d^*x \\ &= \int_{\mathbf{R}^*} e^{-\pi x^2} |x|^{s+1} \, d^*x \\ &= \pi^{-(\frac{s+1}{2})} \Gamma(\frac{s+1}{2}) \end{aligned}$$

where the last line follows by the first computation. Thus again $Z(f,\chi)=L(\chi)$ by definition. But contour integration also shows that

$$\hat{f}(y) = iye^{-\pi y^2}$$

and so

$$Z(\hat{f},\chi^\vee) = i\int_{\mathbf{R}^*} xe^{-\pi x^2} \cdot \frac{x}{|x|} \cdot |x|^{1-s} d^*x = iL(\chi^\vee).$$

Thus for $\chi = \mathrm{sgn}\, |\cdot|^s$ we have $\varepsilon(\chi)=\varepsilon(\chi, \psi, dx)=i$.

CASE TWO: $F=\mathbf{C}$. We take the measure on $\mathbf{C}$ to be $dz d\bar{z} = 2dxdy$, which is twice the ordinary Lebesgue measure and self-dual with respect to our standard complex character

$$\psi(z) = e^{-2\pi i(z+\bar{z})}.$$

Furthermore, we adjust the norm on $\mathbf{C}$ to agree with the module; that is, for purposes of these calculations, set

$$|z| = z\bar{z}.$$

As we have seen above, since $\mathbf{C}^* = \mathbf{R}_+^\times \times S^1$, every character of $\mathbf{C}^*$ takes the form

$$\chi_{s,n} : re^{i\theta} \mapsto r^s e^{in\theta}$$

for some uniquely defined complex s and integral n. Put

$$f_n(z) = \begin{cases} (2\pi)^{-1} \bar{z}^n e^{-2\pi z\bar{z}} & \text{for } n \geq 0 \\ (2\pi)^{-1} z^{-n} e^{-2\pi z\bar{z}} & \text{for } n < 0\,. \end{cases}$$

One can show that the Fourier transform of f_n is then given by

$$\hat{f}_n(z)=(2\pi)^{-1}i^{|n|}f_{-n}(z)$$

for all n. Note finally that $d^*z=(2/r)dr\,d\theta$. We may then compute for n positive or zero:

$$\begin{aligned}
Z(f_n,\chi_{s,n}) &= \int_{\mathbf{C}^*} f_n(z)\chi_{s,n}(z)d^*z \\
&= \frac{1}{2\pi}\int_{\mathbf{C}^*} \bar{z}^n e^{-2\pi z\bar{z}}(z\bar{z})^s e^{in\theta(z)}d^*z \\
&= \frac{1}{\pi}\int_0^{2\pi}\int_0^{\infty} r^n e^{-2\pi r^2} r^{2s}\frac{1}{r}\,dr\,d\theta \\
&= (2\pi)^{-(s+\frac{n}{2})}\int_0^{\infty} e^{-2\pi r^2}(2\pi r^2)^{s+\frac{n}{2}-1}4\pi r\,dr\ .
\end{aligned}$$

The result cries out for the substitution $t=2\pi r^2$, whence

$$\begin{aligned}
Z(f_n,\chi_{s,n}) &= (2\pi)^{-(s+\frac{n}{2})}\int_0^{\infty} e^{-t}t^{s+\frac{n}{2}-1}dt \\
&= (2\pi)^{-(s+\frac{n}{2})}\Gamma(s+\frac{n}{2}) \\
&= L(\chi_{s,n})\ .
\end{aligned}$$

Repeating the calculation for negative n shows that in fact,

$$Z(f_n,\chi_{s,n})=(2\pi)^{-(s+\frac{|n|}{2})}\Gamma(s+\frac{|n|}{2})=L(\chi_{s,n})$$

for all n. Since clearly

$$\chi_{s,n}^{\vee}=\chi_{1-s,-n}$$

it follows from the linearity of this calculation and from the formula for the Fourier transform of f_n given above that

$$Z(\hat{f}_n,\chi_{s,n}^{\vee})=i^{|n|}(2\pi)^{-(1-s+\frac{|n|}{2})}\Gamma(1-s+\frac{|n|}{2})=i^{|n|}L(\chi_{s,n}^{\vee})\ .$$

Consequently,

$$\gamma(\chi_{s,n}) = i^{|n|}\frac{L(\chi_{s,n}^{\vee})}{L(\chi_{s,n})}$$

and

$$\varepsilon(\chi_{s,n}) = i^{|n|}\,.$$

This completes the proof for the complex case.

CASE THREE: F is a non-Archimedean local field. We shall treat only the case of characteristic zero; see Exercise 5 for positive characteristic. Thus we assume that F is a finite extension $\mathbf{Q}_p$ for a fixed rational prime p. We have a standard additive character ψ_p on $\mathbf{Q}_p$ defined by the following composition:

$$\psi_p = [\mathbf{Q}_p \overset{\text{can.}}{\to} \mathbf{Q}_p/\mathbf{Z}_p \to \mathbf{Q}/\mathbf{Z} \overset{e^{2\pi i(\cdot)}}{\to} S^1]\,.$$

(Exercise 3 gives an explicit construction.) This character induces a standard additive character ψ_F on F via the trace map from F to $\mathbf{Q}_p$. Thus for $x \in F$,

$$\psi_F(x) = \psi_p(\mathrm{tr}(x))\,.$$

Note that ψ_F is clearly trivial on $\mathfrak{o}_F$. We know, moreover, that any additive character of F takes the form

$$\psi(x) = \psi_F(zx) = \psi_p(\mathrm{tr}(zx))$$

for some $z \in F$. (Likewise, in positive characteristic we can define a standard character ψ_F in the local case such that ψ_F is trivial on the associated ring of integers; again, see Exercise 3.)

Fix a nontrivial additive character ψ and the corresponding self-dual measure dx. For these calculations, ψ need not be the standard character. Define an integer constant m as follows:

$$m = \inf\{r \in \mathbf{Z} : \psi|_{P^r} = 1\}$$

where P is the unique prime of F, and here we understand P^0 to be $\mathfrak{o}_F$. Note that m is indeed finite because ψ is assumed continuous and takes the value one at zero. We call P^m the *conductor* of ψ. For the trivial character, one customarily takes the conductor to be $\mathfrak{o}_F$.

For a multiplicative character $\chi: F^* \to \mathbf{C}^*$ we define the conductor to be P^n, where $U_n = 1 + P^n$ $(n \geq 0)$ is the largest subgroup of this form on which χ is trivial. In the case that n is zero, we take U_0 to be $\mathfrak{o}_F^{\times}$ and say that χ is *unramified.*

Consider again the trace map $\mathrm{tr}: F \to \mathbf{Q}_p$, which is nondegenerate; indeed, the nondegeneracy of the trace map characterizes finite separable extensions. We can define a subset $\mathfrak{o}'_F$ of F, called the dual of $\mathfrak{o}_F$, as follows:

$$\mathfrak{o}'_F = \{x \in F : \mathrm{tr}(x \cdot \mathfrak{o}_F) \subseteq \mathbf{Z}_p\}.$$

One sees at once that $\mathfrak{o}'_F$ is a $\mathbf{Z}_p$-submodule of F, and since F is a local field, there exists an integer d such that

$$\mathfrak{o}'_F = \pi_F^{-d}\,\mathfrak{o}_F .$$

Note that by construction, the standard character on F has conductor $\mathfrak{o}'_F$, which accordingly has exponent $-d$. We now define $\mathcal{D} = \mathcal{D}_F$, the *different* of F, by

$$\mathcal{D} = (\mathfrak{o}'_F)^{-1} = \pi_F^{d}\,\mathfrak{o}_F .$$

Thus the different of F is the inverse of the dual of $\mathfrak{o}_F$ with respect to the trace map. (See Appendix B, Section 2, and also the exercises from Chapter 4 for more information on the different.)

Write $\chi_{s,n}$ for the map

$$x \mapsto |x|^s\,\omega(x/|x|)$$

where ω is a unitary character of conductor P^n. Certainly every multiplicative character of F is of this form, and while the indices do not completely determine $\chi_{s,n}$, they do suffice to determine the ensuing computations. Now define f by

$$f(x) = \begin{cases} \psi(x) & \text{if } x \in P^{m-n} \\ 0 & \text{otherwise} \end{cases} \tag{7.3}$$

where again P^m is the conductor of ψ. We shall now compute $Z(f, \chi_{s,n})$ separately for n equal to zero and for n positive.

CASE $n=0$. This is a routine calculation. We need only keep in mind that ψ is trivial on its conductor P^m, ω is trivial everywhere, and $P^m - \{0\}$ is the disjoint union of the sets $\pi_F^k\,\mathfrak{o}_F^\times$ for $k \geq m$. Accordingly, we compute

$$Z(f,\chi_{s,n}) = \int_{F^*} f(x)\chi_{s,n}(x)\,d^*x$$

$$= \int_{P^m-\{0\}} |x|^s\,d^*x$$

$$= \mathrm{Vol}(\mathfrak{o}_F^\times, d^*x)\sum_{k\geq m} q^{-ks} \tag{7.4}$$

$$= \mathrm{Vol}(\mathfrak{o}_F^\times, d^*x)\,\frac{q^{-ms}}{1-q^{-s}}$$

$$= q^{-ms}\,\mathrm{Vol}(\mathfrak{o}_F^\times, d^*x)\,L(s,1)$$

where of course, $L(s,1) = L(\chi_{s,0})$.

CASE $n>0$. One sees at once that

$$Z(f,\chi_{s,n}) = \sum_{k\geq m-n} q^{-ks}\int_{\mathfrak{o}_F^\times} \psi(\pi^k u)\omega(u)\,d^*u\ .$$

To resolve this expression, we resurrect in modern form one of the classic constructions of number theory. For any multiplicative character $\omega:\mathfrak{o}_F^\times \to S^1$ and additive character $\lambda:\mathfrak{o}_F \to S^1$, we define the associated *Gauss sum* to be

$$g(\omega,\lambda) = \int_{\mathfrak{o}_F^\times} \omega(u)\lambda(u)\,d^*u\ .$$

Then

$$Z(f,\chi_{s,n}) = \sum_{k\geq m-n} q^{-ks} g(\omega,\psi_{\pi^k})$$

where again $\psi_t(x) = \psi(tx)$.

7-4 LEMMA. *Let ω and λ have conductors P^n and P^r, respectively. Then the following statements hold:*

(i) *If $r<n$, then $g(\omega,\lambda)=0$.*

(ii) *If $r=n$, then $|g(\omega,\lambda)|^2 = c\mathrm{Vol}(\mathfrak{o}_F,dx)\mathrm{Vol}(U_n,d^*x)$.*

(iii) *If $r>n$, then $|g(\omega,\lambda)|^2 = c\mathrm{Vol}(\mathfrak{o}_F,dx)\,[\mathrm{Vol}(U_n,d^*x) - q^{-1}\mathrm{Vol}(U_{r-1},d^*x)]$.*

PROOF. Write $U=\mathfrak{o}_F^\times$ as a disjoint union of cosets modulo $U_r=1+P^r$, and note that $\lambda(a(1+\pi^r b))=\lambda(a)\lambda(\pi^r ab)=\lambda(a)$ by definition of the conductor. Thus

$$g(\omega,\lambda)=\sum_{U/U_r}\lambda(a)\omega(a)\int_{U_r}\omega(u)\,d^*u\ .$$

But if $r<n$, then $\omega|_{U_r}$ is nontrivial, and the indicated integral is zero by the orthogonality of the characters. This proves part (i).

Now suppose that $r\geq n$. We have

$$\begin{aligned}|g(\omega,\lambda)|^2&=\int_U\int_U\omega(xy^{-1})\lambda(x-y)d^*x\,d^*y\\&=\int_U\omega(z)h(z)d^*z\end{aligned}$$

where

$$h(z)=\int_U\lambda(y(z-1))d^*y=c\int_U\lambda(y(z-1))dy\ .$$

(The second equality holds because $c\cdot dx=|x|d^*x$ and $|y|=1$ whenever y lies in the unit group U.) Thus

$$\begin{aligned}h(z)&=c\int_{\mathfrak{o}_F}\lambda(y(z-1))dy-c\int_P\lambda(y(z-1))dy\\&=\begin{cases}c(1-q^{-1})\mathrm{Vol}(\mathfrak{o}_F,dx) & \text{if } v_P(z-1)\geq r\\-cq^{-1}\mathrm{Vol}(\mathfrak{o}_F,dx) & \text{if } v_P(z-1)=r-1\\0 & \text{otherwise.}\end{cases}\end{aligned}$$

From this we get

$$|g(\omega,\lambda)|^2=\begin{cases}c(1-q^{-1})\mathrm{Vol}(\mathfrak{o}_F,dx)\mathrm{Vol}(U,d^*x) & \text{if } 0=r(=n)\\[2ex] c\,\mathrm{Vol}(\mathfrak{o}_F,dx)[\mathrm{Vol}(U_r,d^*x)-q^{-1}\displaystyle\int_{U_{r-1}}\omega(z)d^*z] & \text{if } 0<r\end{cases}$$

and parts (ii) and (iii) now follow at once. ❑

Resuming the computation of $Z(f,\chi_{s,n})$, we deduce from the first part of the lemma and the equation that precedes it that for n positive,

$$Z(f,\chi_{s,n}) = q^{-(m-n)s} g(\omega, \psi_{\pi^{m-n}}). \tag{7.5}$$

But now we see from part (ii) of the lemma that since the conductor of both ω and $\psi_{\pi^{m-n}}$ have exponent n, the second factor on the right-hand side of this equation cannot be zero. Thus in this case $Z(f,\chi_{s,n})$ is essentially an exponential function, with neither zeros nor poles—which is well, because by definition $L(\chi_{s,n})=1$ for $n>0$.

Next we make ready for the other half of the calculation, and for this we need to compute a Fourier transform.

7-5 LEMMA. *For the function f defined by Eq. 7.3, the Fourier transform of f is given as* $\mathrm{Vol}(P^{m-n},dx)$ *times the characteristic function of* $\mathfrak{o}_F$ *for* $n=0$ *and as* $\mathrm{Vol}(P^{m-n},dx)$ *times the characteristic function of* P^n-1 *for* $n>0$.

PROOF. By definition,

$$\hat{f}(y) = \int_F f(x)\psi(xy)\,dx = \int_{P^{m-n}} \psi(x(y+1))\,dx\,.$$

Let $n=0$. Then since the conductor of ψ is P^m, by orthogonality $\hat{f}(y)$ is zero if y does not lie in $\mathfrak{o}_F$. When y does lie in $\mathfrak{o}_F$, then $\hat{f}(y) = \mathrm{Vol}(P^{m-n})$. Now suppose that n is positive. Then if y is not in P^n-1, then $v_P(y+1)\le n-1$, and thus the product $x(y+1)$ occurring in the integrand does not lie in P^m. Accordingly, ψ_{y+1} is a nontrivial character of P^{m-n}, and by orthogonality, $\hat{f}(y)$ is zero. When y does lie in P^n-1, then again $\hat{f}(y) = \mathrm{Vol}(P^{m-n})$. ❑

With this fundamental technical lemma in hand, we are now prepared to compute the value of $Z(\hat{f},\chi^{\vee}_{s,n})$.

CASE $n=0$. Using the last lemma and the by now familiar decomposition of integers of F into the disjoint union of subsets of a given valuation, we find that

$$\begin{aligned} Z(\hat{f},\chi^{\vee}_{s,0}) &= \mathrm{Vol}(P^m,dx) \int_{\mathfrak{o}_F-\{0\}} \chi^{\vee}_{s,0}(y)\,d^*y \\ &= \mathrm{Vol}(P^m,dx)\sum_{k\ge 0} q^{-k(1-s)} \int_{\mathfrak{o}_F^\times} d^*y \\ &= \mathrm{Vol}(P^m,dx)\,\mathrm{Vol}(\mathfrak{o}_F^\times,d^*x)\, \frac{1}{1-q^{-(1-s)}} \\ &= \mathrm{Vol}(P^m,dx)\,\mathrm{Vol}(\mathfrak{o}_F^\times,d^*x)\, L(\chi^{\vee}_{s,0})\,. \end{aligned}$$

Thus we find from this and Eq. 7.4 that

$$\gamma(\chi_{s,0}) = q^{ms}\,\mathrm{Vol}(P^m, dx)\frac{L(\chi^\vee_{s,0})}{L(\chi_{s,0})}$$

and

$$\varepsilon(\chi_{s,0}, \psi, dx) = q^{ms}\,\mathrm{Vol}(P^m, dx)\,.$$

CASE $n>0$. Again the lemma applies, and we have at once that

$$\begin{aligned} Z(\hat{f}, \chi^\vee_{s,n}) &= \mathrm{Vol}(P^{m-n}, dx) \int_{P^n-1} \overline{\omega}(u)d^*u \\ &= \mathrm{Vol}(P^{m-n}, dx) \int_{1+P^n} \overline{\omega}(-u)d^*u \\ &= \mathrm{Vol}(P^{m-n}, dx)\,\mathrm{Vol}(1+P^n, d^*x)\,\omega(-1) \end{aligned}$$

since the conductor of ω is identical to that of its conjugate. The result is a constant, as it should be, since $L(\chi^\vee_{s,n}) = 1$ for n positive. Accordingly, it follows from Eq. 7.5 that

$$\varepsilon(\chi_{s,n}, \psi, dx) = \gamma(\chi_{s,n}, \psi, dx) = \frac{q^{(m-n)s}\,\mathrm{Vol}(P^{m-n}, dx)\,\mathrm{Vol}(1+P^n, d^*x)\,\omega(-1)}{g(\omega, \psi_{\pi^{m-n}})}\,.$$

Now one sees easily that

$$\overline{g(\omega, \psi_{\pi^{m-n}})} = \omega(-1)g(\overline{\omega}, \psi_{\pi^{m-n}})$$

and since the conductor of $\psi_{\pi^{m-n}}$ is P^n, by combining the formulas above for the epsilon factor with part (ii) of Lemma 7-4, we get the following compact formula:

$$\varepsilon(\chi_{s,n}, \psi, dx) = \frac{1}{c} q^{(m-n)(s-1)} g(\overline{\omega}, \psi_{\pi^{m-n}})\ .$$

Here we have also used that $\mathrm{Vol}(P^{m-n}) = q^{n-m} \cdot \mathrm{Vol}(\mathfrak{o}_F)$.

To conclude our analysis, we observe that in all three cases the poles of $Z(f,\chi)$ are given by the zeros of the now clearly meromorphic function

$$\gamma(\chi, \psi, dx) = \varepsilon(\chi, \psi, dx)\frac{L(\chi^\vee)}{L(\chi)}$$

because the regions of absolute convergence of $Z(f,\chi)$ and $Z(\hat{f},\chi^\vee)$ are, respectively, $\mathrm{Re}(s)>0$ and $\mathrm{Re}(s)<1$. Moreover, the zeros of γ must coincide with the poles of $L(\chi)$, since $L(\chi)$ and $L(\chi^\vee)$ have no zeros. This finishes the proof of Theorem 7-2. ❑

The Root Number

Let F be a non-Archimedean local field of characteristic zero. From Exercise 7 below we have the following result:

> *Suppose that* $\psi(x)=\psi_p(\mathrm{tr}(x))$, *the standard nontrivial character of F. Then the associated self-dual measure dx on F is the one that satisfies the relation* $\mathrm{Vol}(\mathfrak{o}_F,dx)=N(\mathcal{D}_F)^{-1/2}=q^{-d/2}$, *where* $\mathcal{D}_F=\pi_F^d\,\mathfrak{o}_F$ *is the different of F, as described above.*

For a multiplicative character ω, one defines the *root number* $W(\omega)$ by

$$W(\omega)=\varepsilon(\omega|\cdot|^{1/2},\psi,dx)\,.$$

One can show (see Exercise 9 below) that $W(\omega)$ is of absolute value 1. If the conductor of ω has exponent n and λ is any additive character whose conductor also has exponent n, one sees readily that

$$g(\overline{\omega},\lambda)=c\,\mathrm{Vol}(P^n)\sum_{x\in U/U_n}\overline{\omega}(x)\lambda(x)\,.$$

The sum on the right is the usual Gauss sum. Now suppose that ψ is the standard character and dx the self-dual measure. Then it follows immediately from the ε-formula above and the preceding expansion that

$$W(\omega)=q^{-n/2}\sum_{x\in U/U_n}\overline{\omega}(x)\psi(x\pi^{-(d+n)})\,. \tag{7.6}$$

7.2 The Riemann-Roch Theorem

A basic result of abelian harmonic analysis, both in the classical and adelic settings, is the Poisson summation formula, which relates the averages over a lattice of a nice function and its Fourier transform. The Riemann-Roch theorem provides a nontrivial and valuable extension. In the function field case, it can be interpreted as giving the "usual" Riemann-Roch theorem for curves over $\mathbf{F}_q$, whence its name.

We begin with some notation. Let K be a global field. Then define

$$S(\mathbf{A}_K)=\bigotimes_v{}'\,S(K_v)$$

where the restricted tensor product of the Schwartz-Bruhat spaces $S(K_v)$ consists of functions of the form

$$f = \otimes f_v : f_v \in S(K_v)\,\forall v \text{ and } f_v|_{\mathfrak{o}_v} = 1, \text{ for almost all } v\,.$$

We shall call such an f an *adelic Schwartz-Bruhat function*; in this case it makes sense to write

$$f(x) = \prod_v f_v(x_v)$$

for all $x=(x_v)\in\mathbf{A}_K$. Let dx denote a Haar measure on $\mathbf{A}_K$ and define $L^2(\mathbf{A}_K)$ using this measure. It is easy to see that $S(\mathbf{A}_K)$ is dense in $L^2(\mathbf{A}_K)$.

Fix a nontrivial (continuous) unitary character ψ on $\mathbf{A}_K$ such that $\psi|_K=1$. (See Exercises 4 and 6 for the existence of such characters.) Define the adelic Fourier transform on any $f\in S(\mathbf{A}_K)$ by

$$\hat{f}(y) = \int_{\mathbf{A}_K} f(x)\psi(xy)dx\,.$$

Here we normalize dx to be the self-dual measure for ψ. In Exercise 12 below we shall deduce that the mapping $f \mapsto \hat{f}$ defines an automorphism of $S(\mathbf{A}_K)$ that moreover extends to an isometry of $L^2(\mathbf{A}_K)$.

We are interested in functions on $\mathbf{A}_K$ that are invariant with respect to translation by elements of K. One example is ψ. An obvious approach to finding others is to take an average over K. To elaborate, set

$$\tilde{\varphi}(x) = \sum_{\gamma\in K}\varphi(\gamma + x)$$

for $\varphi\in S(\mathbf{A}_K)$. When this function is convergent for all x, we see that for all $\delta\in K$ it satisfies the relation

$$\tilde{\varphi}(\delta + x) = \sum_{\gamma\in K}\varphi(\gamma+\delta+x) = \sum_{\gamma'\in K}\varphi(\gamma'+x) = \tilde{\varphi}(x)$$

where $\gamma'=\gamma+\delta$. Thus $\tilde{\varphi}(\delta+x)=\tilde{\varphi}(x)$, as desired.

DEFINITION. Let f be complex-valued on $\mathbf{A}_K$ such that both $\tilde{f}$ and $\tilde{\hat{f}}$ are normally convergent; that is, both are absolutely and uniformly convergent on compact subsets. Then we say that f is *admissible*.

7-6 LEMMA. *Every function $f \in S(\mathbf{A}_K)$ is admissible.*

PROOF. Let $f \in S(\mathbf{A}_K)$. We have to show the absolute and uniform convergence of f over any compact subset C of $\mathbf{A}_K$. By enlarging C, we may assume without loss of generality that C takes the form

$$C_\omega \times \prod_{v \in S} P_v^{n_v} \times \prod_{v \notin S} \mathfrak{o}_v$$

where S is a finite set of finite places including those at which $f|_{\mathfrak{o}_v} \neq 1$,

$$C_\omega = \prod_{v \in S_\omega} C_v$$

is a compact set in the product $K_\omega = \Pi K_v$ taken over the set S_ω of infinite places, and n_v is an integer for all $v \in S$. We may enlarge S to contain S_ω and assume that f_v is the characteristic function of $P_v^{m_v}$ for all $v \in S - S_\omega$. Note that such functions generate $S(\mathbf{A}_K)$. Define a fractional ideal I in $\mathfrak{o}_K$ by

$$I = \prod_{v \in S - S_\omega} P_v^{k_v}$$

where $k_v = \inf\{n_v, m_v\}$. Suppose that $f(\gamma + z) \neq 0$ for some $z \in C$ and $\gamma \in K$. Then γ lies in $P_v^{k_v}$ for all $v \in S - S_\omega$, and in $\mathfrak{o}_v$ for all $v \notin S$. Thus

$$|\tilde{f}(z)| \leq \sum_{\gamma \in I} |f_\omega(\gamma + z_\omega)|$$

where

$$f_\omega = \prod_{v \in S_\omega} f_v \in S(K_\omega) \quad \text{and} \quad z_\omega = (z_v)_{v \in S_\omega}.$$

But I is a discrete subgroup of K_ω (this follows, for instance, from the discreteness of K in $\mathbf{A}_K$), and the Schwartz-Bruhat function f_ω has a uniform absolute bound over the compact set C_ω, with the further property that the value of $|f_\omega(\gamma + z_\omega)|$ decreases rapidly with z_ω in the number field case, while f_ω has compact, hence finite, support in the function field case. Thus for a number field, the number of γ that occur in any shell of radius B and thickness ΔB can grow at most as a power of B, while $|f_\omega|$ goes to zero faster than any polynomial; for a function field, the number of terms in the summation is finite. The normal convergence of f follows. Since this extends at once to its Fourier transform, which also lies in $S(\mathbf{A}_K)$, the proof is complete. ❑

7-7 THEOREM. (Poisson Summation Formula) *Let* $f \in S(\mathbf{A}_K)$. *Then* $\tilde{f} = \tilde{\hat{f}}$; *that is,*

$$\sum_{\gamma \in K} f(\gamma + x) = \sum_{\gamma \in K} \hat{f}(\gamma + x)$$

for all $x \in \mathbf{A}_K$.

PROOF. Every K-invariant function φ on $\mathbf{A}_K$ induces a function, again denoted φ, on $\mathbf{A}_K/K$. For all $z \in K$ we set

$$\hat{\varphi}(z) = \int_{\mathbf{A}_K/K} \varphi(t)\psi(tz)\overline{dt}$$

where $\overline{dt}$ is the quotient measure on $\mathbf{A}_K/K$ induced by dt on $\mathbf{A}_K$. This is to say that $\overline{dt}$ is characterized by the relation

$$\int_{\mathbf{A}_K/K} \tilde{f}(t)\,\overline{dt} = \int_{\mathbf{A}_K/K} (\sum_{\gamma \in K} f(\gamma + t))\overline{dt} = \int_{\mathbf{A}_K} f(t)\,dt$$

for all continuous functions f on $\mathbf{A}_K$ with appropriate convergence properties. (The integration variable t, as it occurs on the left and in the middle, takes values in the quotient group $\mathbf{A}_K/K$; nonetheless, the indicated expressions are well-defined.) We shall need two lemmas.

7-8 LEMMA. *For every function f in* $S(\mathbf{A}_K)$, *we have*

$$\hat{f}|_K = \hat{\tilde{f}}|_K .$$

PROOF. Fix $z \in K$. By definition,

$$\begin{aligned}\hat{\tilde{f}}(z) &= \int_{\mathbf{A}_K/K} \tilde{f}(t)\psi(tz)\overline{dt} \\ &= \int_{\mathbf{A}_K/K} (\sum_{\gamma \in K} f(\gamma + t))\psi(tz)\,\overline{dt}\,.\end{aligned}$$

Since we assume that the unitary character ψ has the property $\psi|_K = 1$, we have that

$$\psi(tz) = \psi((\gamma + t)z)$$

for all $\gamma\in K$. Accordingly, by definition of the quotient measure (relative to the counting measure on K) it follows that

$$\begin{aligned}\hat{\tilde{f}}(z) &= \int_{\mathbf{A}_K/K} \Big(\sum_{\gamma\in K} f(\gamma+t)\psi((\gamma+t)z)\Big)\overline{dt} \\ &= \int_{\mathbf{A}_K} f(t)\psi(tz)dt \\ &= \hat{f}(z)\end{aligned}$$

and this completes the proof. ❑

7-9 LEMMA. *Let $f\in S(\mathbf{A}_K)$. Then for every $x\in K$, we have*

$$\tilde{f}(x) = \sum_{\gamma\in K}\hat{\tilde{f}}(\gamma)\overline{\psi}(\gamma x).$$

PROOF. By the previous lemma, $\hat{f}|_K = \hat{\tilde{f}}|_K$ on K. Hence the summation

$$\sum_{\gamma\in K}\hat{\tilde{f}}(\gamma)\overline{\psi}(\gamma x)$$

is normally convergent. In particular,

$$\sum_{\gamma\in K}|\hat{\tilde{f}}(\gamma)| < \infty$$

and so the Fourier inversion formula applies. (Since the Pontryagin dual of the quotient $\mathbf{A}_K/K$ is K itself under the discrete topology, the indicated summations correspond to the appropriate integrals.) The assertion of the lemma follows. ❑

We are now prepared to deduce the Poisson summation formula. Indeed, if we put $x=0$ into the second lemma and then apply the first, we have on the one hand that

$$\tilde{f}(0) = \sum_{\gamma\in K}\hat{\tilde{f}}(\gamma) = \sum_{\gamma\in K}\hat{f}(\gamma).$$

But on the other hand, by definition,

$$\tilde{f}(0) = \sum_{\gamma \in K} f(\gamma)$$

and this suffices. □

It is of interest in number theory to understand the average

$$\sum_{\gamma \in K} f(\gamma x)$$

for an idele x. [Note that the absolute convergence of this summation follows from that of $\sum f(\gamma)$, which is implicit in the admissibility of f.] One cannot get this information from the previous theorem, and one needs instead the following stronger result.

7-10 THEOREM. (Riemann-Roch) *Let x be an idele of K and let f be an element of $S(\mathbf{A}_K)$. Then*

$$\sum_{\gamma \in K} f(\gamma x) = \frac{1}{|x|} \sum_{\gamma \in K} \hat{f}(\gamma x^{-1}) \ .$$

PROOF. Fix $x \in \mathbf{A}_K$, and for arbitrary $y \in \mathbf{A}_K$, define $h(y) = f(yx)$. Clearly, $h \in S(\mathbf{A}_K)$. Thus, by the Poisson summation formula,

$$\sum_{\gamma \in K} h(\gamma) = \sum_{\gamma \in K} \hat{h}(\gamma) \ .$$

But

$$\begin{aligned} \hat{h}(\gamma) &= \int_{\mathbf{A}_K} f(yx)\psi(\gamma y)dy \\ &= \frac{1}{|x|} \int_{\mathbf{A}_K} f(y)\psi(\gamma y x^{-1})dy \\ &= \frac{1}{|x|} \hat{f}(\gamma x^{-1}) . \end{aligned}$$

The theorem now follows immediately. □

The Riemann-Roch Theorem for Algebraic Curves

When K is a function field in one variable over $\mathbf{F}_q$, the previous theorem can be interpreted to yield the perhaps more familiar Riemann-Roch theorem of algebraic geometry. We shall explain this after some preliminaries.

A *divisor* on K is a formal linear combination

$$D = \sum_{v} n_v v$$

where the sum runs over all places v of K and each coefficient n_v is an integer that is zero for almost all v. The divisors on K naturally form an additive group, denoted Div(K). The *degree* of a divisor $D = \sum n_v v$ is defined by

$$\deg(D) = \sum_{v} n_v \deg(v)$$

where deg(v) is the degree (over $\mathbf{F}_q$) of the residue field $\mathbf{F}_{q_v}$ at v. Thus

$$q_v = N(v) = q^{\deg(v)} .$$

Since $\deg(D+D') = \deg(D) + \deg(D')$, we see that the degree map defines a homomorphism $\deg : \mathrm{Div}(K) \to \mathbf{Z}$, the kernel of which is denoted $\mathrm{Div}^0(K)$, the group of *divisors of degree zero.*

Given any $f \in K^*$, we can associate a divisor, called a *principal divisor*, by setting

$$\mathrm{div}(f) = \sum_{v} v(f) v$$

where $v(f)$ of course denotes the valuation of f at v. [In geometry, it is customary to write $\mathrm{ord}_v(f)$ rather than $v(f)$.] Since $v(f)$ can be nonzero only at a finite number of places, div(f) is a bona fide divisor. Moreover, it is obvious that $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$. The quotient $\mathrm{Div}(K)/\mathrm{div}(K^*)$ is denoted Pic(K) and called the *Picard group* of K. Elements of Pic(K) are called *divisor classes.*

Recall that Artin's product formula says that for all $f \in K^*$,

$$|f|_{\mathbf{A}_K} = \prod_{v} |f|_v = 1 .$$

But

$$|f|_v = q_v^{-v(f)} = q^{-v(f)\deg(v)}$$

for all v, so

$$\deg(\mathrm{div}(f)) = \sum_{v} v(f) \deg(v) = 0 .$$

Thus we see that $\mathrm{div}(K^*) \subseteq \mathrm{Div}^0(K)$.

Now suppose that $\text{div}(f)=\text{div}(g)$ for f and g in K^*. Then $\text{div}(f/g)=0$, and the quotient $\alpha=f/g$ is a unit of $\mathfrak{o}_v$ for *all* v. From Chapter 5, Exercise 5, we know that any such α must lie in $\mathbf{F}_q{}^*$. To summarize, we have the following exact sequence of groups:

$$1 \to \mathbf{F}_q^* \to K^* \overset{\text{div}}{\to} \text{Div}^0(K) \to \text{Pic}^0(K) \to 0$$

where $\text{Pic}^0(K)$, the *Picard group of degree zero*, of course denotes the quotient $\text{Div}^0(K)/\text{div}(K^*)$. Clearly, deg induces a homomorphism, again denoted deg, on $\text{Pic}(K)$, with kernel $\text{Pic}^0(K)$. Elements of $\text{Pic}^0(K)$ are called *divisor classes of degree zero*.

We next introduce the partial ordering on $\text{Div}(K)$ defined by

$$D = \sum_v n_v v \geq D' = \sum_v n'_v v \quad \text{if} \quad n_v \geq n'_v \ \forall v .$$

With this, to each divisor D one may associate the following *linear system* of D:

$$L(D) = \{0\} \cup \{f \in K^* : \text{div}(f) \geq -D\} .$$

Since $\text{div}(f)$ has degree zero for $f \in K^*$, we have at once that $L(0)=\mathbf{F}_q$. One may further deduce from the Artin product formula that $L(D)=\{0\}$ if $\deg(D)<0$.

Note that $L(D)$ is clearly closed under scalar multiplication from $\mathbf{F}_q$. Moreover, it is closed under addition by the ultrametric inequality:

$$v(f+g) \geq \inf\{v(f), v(g)\} .$$

Hence $L(D)$ is in fact a vector space over $\mathbf{F}_q$, and one writes $l(D)$ for the dimension of this space. One sees immediately from our previous observations that $l(0)=1$ and $l(D)=0$ if $\deg(D)<0$. It is not *a priori* clear, however, that in general this number is finite.

7-11 PROPOSITION. *For any divisor D, the number l(D) is finite.*

PROOF. The first step is to extend the divisor map to ideles. Accordingly, we define

$$\begin{aligned} \text{div} : \mathbf{I}_K &\to \text{Div}(K) \\ (x_v) &\mapsto \sum_v v(x_v) v . \end{aligned}$$

It is easy to see that this extended map is surjective. Moreover, we have the following set of equalities:

$$\mathrm{Ker}(\mathrm{div}) = \prod_v \mathfrak{o}_v^\times = \mathbf{I}_{K,\varnothing} \qquad \mathbf{I}_K/K^*\mathbf{I}_{K,\varnothing} = \mathrm{Pic}(K)$$

$$\mathrm{div}(\mathbf{I}_K^1) = \mathrm{Div}^0(K) \qquad \mathbf{I}_K^1/K^*\mathbf{I}_{K,\varnothing} = \mathrm{Pic}^0(K)$$

Next let $f=\otimes_v f_v \in S(\mathbf{A}_K)$ be defined by requiring that each component function f_v be the characteristic function on $\mathfrak{o}_v$. Given any divisor $D=\sum n_v v$, we may associate an idele $x(D)$ such that $v(x(D)_v)=n_v$ for all v. Then, by construction, we have for all $\gamma\in K^*$ that

$$f(\gamma x(D)) = \begin{cases} 1 & \text{if } v(\gamma x(D)_v) \geq 0 \ \forall v \\ 0 & \text{otherwise.} \end{cases}$$

In other words, for nonzero γ, we have that $f(\gamma x(D))$ is nonzero if and only if $\gamma\in L(D)$. Note also that $f(0)=1$.

Since $f\in S(\mathbf{A}_K)$, f is admissible, as defined previously, and accordingly, the following sum converges:

$$\sum_{\gamma\in K} f(\gamma x(D)) .$$

But from our analysis above of $f(\gamma x(D))$ as a function of γ, we see that this sum is exactly $\mathrm{Card}(L(D))=q^{l(D)}$. Hence $l(D)$ is finite, as claimed. ❑

7-12 THEOREM. (Riemann-Roch, Geometric Form) *Let K be a function field in one variable over $\mathbf{F}_q$. Then there exists an integer $g\geq 0$ (called the* genus *of K) and a divisor $\mathcal{K}$ of degree $2g-2$ (called the* canonical divisor *of K), such that*

$$l(D) - l(\mathcal{K}-D) = \deg(D) - g + 1$$

for every divisor D.

Before deducing this from the earlier, harmonic analysis version, of the Riemann-Roch theorem, let us note two important consequences.

7-13 COROLLARY. *If $\deg(D)>2g-2$, then $l(D)=\deg(D)-g+1$. In particular, if K is a rational function field (that is, if K has genus zero), then for any pair of distinct places v and v', there exists a function $f\in K^*$ with a simple zero at v and a simple pole at v'.*

PROOF. Since $\deg(D)>2g-2=\deg(\mathcal{K})$, $\deg(\mathcal{K}-D)<0$, and, by an earlier observation, $l(\mathcal{K}-D)=0$. So by the Riemann-Roch formula, $l(D)=\deg(D)-g+1$. If, moreover, $g=0$ and v and v' are distinct places, consider the divisor $D=v-v'$.

We may assume that $\deg(v) \geq \deg(v')$, whence $\deg(D) \geq 0$ and so $l(D) \geq 1$. Thus by definition there exists a nonzero $f \in L(D)$ that satisfies the assertion. ❑

7-14 COROLLARY. *For the canonical divisor $\mathcal{K}$ we have that $l(\mathcal{K}) = g$.*

PROOF. This follows at once from the special case $D=0$, since clearly, $\deg(0)=0$, and as we have seen, $l(0)=1$. ❑

PROOF OF THEOREM. Pick any nontrivial character $\psi: \mathbf{A}_K \to S^1$ that is trivial on K. (For instance, the standard character; see Exercise 6.) At each place v, let the conductor of ψ_v be $P_v^{m_v}$. Since m_v is zero for almost all v, we get a divisor by setting

$$\mathcal{K} = -\sum_v m_v v \ .$$

One knows also that if ψ' is another nontrivial character of $\mathbf{A}_K$ that is trivial on K, then there exists $\alpha \in K^*$ such that $\psi'(x) = \psi(\alpha x)$ for all $x \in \mathbf{A}_K$. Moreover, one checks easily that if the divisor $\mathcal{K}'$ is constructed relative to ψ', then

$$\mathcal{K}' = \mathcal{K} + \operatorname{div}(\alpha)$$

and thus $\mathcal{K}$ is uniquely determined modulo principal divisors.

Now let $f = \otimes_v f_v \in S(\mathbf{A}_K)$ be defined as above, so that again each component function f_v is the characteristic function on $\mathfrak{o}_v$. We have already seen that for any divisor $D = \sum n_v v$,

$$q^{l(D)} = \sum_{\gamma \in K} f(\gamma x(D))$$

with $x(D)$ defined as above. This is one side of the identity given in the earlier version of the Riemann-Roch theorem (Theorem 7-10). Note also that

$$|x(D)|^{-1} = \prod_v q_v^{n_v} = q^{(\sum_v n_v \deg(v))} = q^{\deg(D)} .$$

So in light of the previous version, it remains only to show that

$$\sum_{\gamma \in K} \hat{f}(\gamma x(D)^{-1}) = q^{l(\mathcal{K}-D)-g+1} \ . \tag{7.7}$$

Recall that the Fourier transform is taken relative to the self-dual measure dx on $\mathbf{A}_K$ defined by ψ. It follows from Exercise 7 below that for all v,

$$\hat{f}_v = N(P_v^{m_v})^{1/2} \cdot \text{ the characteristic function of } P_v^{m_v}.$$

Note that

$$N(P_v^{m_v})^{1/2} = q_v^{+m_v/2} = q^{+\deg(v)m_v/2}$$

so that

$$\prod_v N(P_v^{m_v})^{1/2} = q^{-\deg(\mathcal{K})/2} = q^{1-g} .$$

Thus we have for all $\gamma \in K^*$ that

$$\hat{f}(\gamma x(D)^{-1}) = \begin{cases} q^{1-g} & \text{if } v(\gamma) \geq m_v + n_v \\ 0 & \text{otherwise} \end{cases}$$

and Eq. 7.7 follows at once by definition of $l(\mathcal{K}-D)$.

Note that the formula in the theorem shows at once that g must be an integer, which, as we have seen above, must be $l(\mathcal{K})$. Thus g is indeed a nonnegative integer, as asserted. ❑

REMARK. One learns in basic algebraic geometry that given any function field K over $\mathbf{F}_q$ as above, there is a smooth projective curve X defined over $\mathbf{F}_q$ such that K identifies with the field of rational functions on X. Thus the Riemann-Roch theorem provides valuable geometric insight into X.

7.3 The Global Functional Equation

Let K again be a global field with integers $\mathfrak{o}_K$ and different $\mathcal{D}=\mathcal{D}_K$. Note that the different is defined just as in the local case, but here it is not generated by a power of a uniformizing parameter. (See Appendix B, Section 2.) The local versions of the integers and different at a finite prime P will be denoted $\mathfrak{o}_P$ and $\mathcal{D}_P$, and in fact, the global different is determined by these local versions.

We shall now construct a standard character for the adele group $\mathbf{A}_K$. At each place v of K, let ψ_v denote the standard character and dx_v the associated self-dual measure. We recall from Section 7.1 that for a number field K, these characters are given explicitly by

$$\psi_v(x) = \begin{cases} \psi_p(\mathrm{tr}(x)) & v \text{ finite, } v|p \\ e^{-2\pi i \mathrm{tr}(x)} & v \text{ infinite} \end{cases}$$

where tr denotes the trace map from K_v to $\mathbf{Q}_v$, and ψ_p is the familiar composition $\mathbf{Q}_p \to \mathbf{Q}_p/\mathbf{Z}_p \to \mathbf{Q}/\mathbf{Z} \to S^1$. (Refer to Exercises 3 and 5 for the function field case.) Now set

$$\psi_K(x) = \prod_v \psi_v(x_v)$$

for all adeles $x=(x_v)$. Then ψ_K is well-defined, because $\psi_v=1$ on $\mathfrak{o}_v$ for almost all v, and hence ψ_K is a nontrivial character. Moreover, if F denotes either $\mathbf{Q}$ or $\mathbf{F}_q(t)$ depending upon whether we are dealing with a number field or a function field, the standard character on $\mathbf{A}_K$ clearly factors through the trace map from $\mathbf{A}_K$ to $\mathbf{A}_F$ defined by

$$\begin{aligned} \mathrm{tr}:\mathbf{A}_K &\to \mathbf{A}_F \\ (x_v)_v &\mapsto (\sum_{v|u} \mathrm{tr}_{K_v/F_u}(x_v))_u \end{aligned}$$

where u ranges over all of the places of F. This is to say that

$$\psi_K(x) = \psi_F(\mathrm{tr}(x))$$

for all adeles x of K.

As in the local case, we have a continuous homomorphism

$$\begin{aligned} \mathbf{A}_K &\to \hat{\mathbf{A}}_K \\ y &\mapsto \psi_{K,y} \end{aligned}$$

where $\psi_{K,y}(x)=\psi_K(yx)$ and the product yx is taken componentwise. One shows easily that the given map is an isomorphism of topological groups. We record this and related elementary facts about the characters of the adele group in the following result, the proof of which we leave as an exercise.

7-15 Proposition. *Let K be a global field with standard character ψ_K on the group $\mathbf{A}_K$. Then the following four assertions hold:*

(i) *The group $\mathbf{A}_K$ is self-dual by the isomorphism $y \mapsto \psi_{K,y}$.*

(ii) *ψ_K is trivial on K and hence induces a character on $\mathbf{A}_K/K$.*

(iii) *The Pontryagin dual of $\mathbf{A}_K/K$ (respectively, K) may be naturally identified with K (respectively, $\mathbf{A}_K/K$). Explicitly, this can be realized by the map that sends $x \in K$ to $\psi_{K,x} \in (\mathbf{A}_K/K)^\wedge$. Hence by the self-duality of the full adele group, the translation $\psi_{K,y}$ of ψ_K is trivial on K if and only if $y \in K$.*

(iv) *If ψ is any character of $\mathbf{A}_K/K$, then ψ_v has conductor $\mathfrak{o}_v$ for almost all places v of K.* ❑

Let dx denote the Haar measure on $\mathbf{A}_K$ defined by the product measure $\prod_v dx_v$ on $\prod_v K_v$. One knows from Section 5.1 that this measure is self-dual with re-

spect to our standard character ψ_K, and one can show easily that dx moreover satisfies the relation

$$d(ax) = |a|\,dx$$

for all ideles $a \in \mathbf{I}_K = \mathrm{Aut}(\mathbf{A}_K)$.

The Global Zeta Function

Let χ denote any $\mathbf{C}^*$-valued character of $\mathbf{I}_K$ that is trivial on K^*; in other words, an idele-class character. For $f \in S(\mathbf{A}_K)$, we define the *global zeta function*

$$Z(f,\chi) = \int_{\mathbf{I}_K} f(x)\chi(x)\,d^*x \ .$$

A word about the normalization of d^*x, which again is induced by the product measure $\prod_v d^*x_v$ on $\prod_v K_v{}^*$: for each non-Archimedean place v, it will be convenient for us to take the corresponding constant factor $c = c_v$ (see Section 7.1) such that

$$d^*x_v = \frac{q_v}{q_v - 1} \cdot \frac{dx_v}{|x_v|} \ .$$

We do this so that $\mathfrak{o}_v^\times$ will get measure $(N(\mathcal{D}_v))^{-1/2} = q^{-d_v/2}$. Note again that $d_v = 0$ for almost all v.

One shows easily that $Z(f,\chi)$ is normally convergent in $\sigma = \mathrm{Re}(s) > 1$, where χ has factorization $\mu|\cdot|^s$ with μ unitary, and that it defines a holomorphic function there. Define $\chi^\vee$ to be $\chi^{-1}|\cdot|$, as in the local case.

7-16 THEOREM. (Meromorphic Continuation and Functional Equation) $Z(f,\chi)$ *extends to a meromorphic function of s and satisfies the functional equation*

$$Z(f,\chi) = Z(\hat{f},\chi^\vee).$$

The extended function $Z(f,\chi)$ is in fact holomorphic everywhere except when $\mu = |\cdot|^{-i\tau}$, $\tau \in \mathbf{R}$, in which case it has simple poles at $s = i\tau$ and $s = 1 + i\tau$ with corresponding residues given by

$$-\mathrm{Vol}(C_K^1)f(0) \quad \text{and} \quad \mathrm{Vol}(C_K^1)\hat{f}(0)$$

respectively.

Here, as in Chapter 5, the symbol C_K^1 denotes the quotient $\mathbf{I}_K^1/K^*$, which is the compact part of the idele class group $\mathbf{I}_K/K^*$. The volume of C_K^1 is taken relative to the quotient measure on C_K defined by d^*x and the counting measure on K^*. The computation of Vol(C_K^1) will be done in Section 7.5.

REMARK. While we implicitly state and prove this result with respect to the standard character—which is all we shall need for the next section—it remains true for an arbitrary adele class character ψ with the proviso that the associated measure remains self-dual to ψ.

PROOF. If K is a number field, we may write, for any χ of exponent greater than one,

$$Z(f,\chi)=\int_0^\infty Z_t(f,\chi)\frac{1}{t}\,dt$$

where

$$Z_t(f,\chi)=\int_{\mathbf{I}_K^1} f(tx)\chi(tx)\,d^*x\ .$$

(Here the product tx takes place in a fixed infinite component of x.) For K a function field, we have

$$Z(f,\chi)=\sum_{|t|_\infty=0}^{\infty} Z_t(f,\chi)$$

with $Z_t(f,\chi)$ as above. We will establish a functional equation for $Z_t(f,\chi)$ by using the Riemann-Roch theorem. To be precise, we assert the following:

7-17 PROPOSITION. *The function $Z_t(f,\chi)$ satisfies the relation*

$$Z_t(f,\chi)=Z_{t^{-1}}(\hat{f},\chi^\vee)+\hat{f}(0)\int_{C_K^1}\chi^\vee(x/t)\,d^*x\ -\ f(0)\int_{C_K^1}\chi(tx)\,d^*x\ .$$

PROOF. Since C_K^1 is the quotient $\mathbf{I}_K^1/K^*$, we have

$$Z_t(f,\chi)=\int_{C_K^1}\Big(\sum_{a\in K^*}f(atx)\Big)\chi(tx)\,d^*x\ =\ \int_{C_K^1}\chi(tx)\,d^*x\sum_{a\in K^*}f(atx)$$

where the summation should now be regarded as the second factor of an iterated integral. We have also used the hypothesis that $\chi=1$ on K^*.

To apply the Riemann-Roch theorem, we need to sum over K, not K^*. This leads us to consider the following expression:

$$Z_t(f,\chi)+f(0)\int_{C_K^1}\chi(tx)\,d^*x$$

which equals

$$\int_{C_K^1}\chi(tx)\,d^*x\sum_{a\in K}f(atx).$$

Via the Riemann-Roch theorem, we may replace the right-hand factor by

$$\frac{1}{|tx|}\sum_{a\in K}\hat{f}(at^{-1}x^{-1}).$$

Thus

$$\begin{aligned}Z_t(f,\chi)+f(0)\int_{C_K^1}\chi(tx)\,d^*x &= \int_{C_K^1}\frac{\chi(tx)}{|tx|}\,d^*x\sum_{a\in K}\hat{f}(at^{-1}x^{-1})\\ &= \int_{C_K^1}|t^{-1}x|\,\chi(tx^{-1})\,d^*x\sum_{a\in K}\hat{f}(at^{-1}x)\end{aligned}$$

where in the second line we have replaced x by x^{-1}. But one shows easily that this equals

$$Z_{t^{-1}}(\hat{f},\chi^\vee)+\hat{f}(0)\int_{C_K^1}\chi^\vee(x/t)\,d^*x$$

since $\chi^\vee=\chi^{-1}|\cdot|$. The formula now follows. ❑

We return to the proof of Theorem 7-16. Suppose that K is a number field. Then we may write

$$Z(f,\chi)=\int_0^1 Z_t(f,\chi)\frac{1}{t}\,dt+\int_1^\infty Z_t(f,\chi)\frac{1}{t}\,dt. \tag{7.8}$$

The second integral is simply

$$\int_{\{x\in\mathbf{I}_K:|x|\geq 1\}} f(x)\chi(x)\,d^*x$$

which converges normally for all s. Indeed, the convergence is better for small σ, and since we know it converges for $\sigma>1$, it must do so everywhere. But also

$$\int_0^1 Z_t(f,\chi)\frac{1}{t}dt = \int_0^1 Z_{t^{-1}}(\hat{f},\chi^\vee)\frac{1}{t}dt + E \tag{7.9}$$

where the correction term is given from the previous proposition by

$$E = \int_0^1 \left[\hat{f}(0)\chi^\vee(t^{-1})\int_{C_K^1}\chi^\vee(x)d^*x - f(0)\chi(t)\int_{C_K^1}\chi(x)d^*x \right]\frac{1}{t}dt.$$

Via the substitution of t^{-1} for t, we find that

$$\int_0^1 Z_{t^{-1}}(\hat{f},\chi^\vee)\frac{1}{t}dt = \int_1^\infty Z_t(\hat{f},\chi^\vee)\frac{1}{t}dt$$

and hence this integral is convergent for all σ, by the argument above. It remains to analyze E. By the orthogonality of the characters, however, both

$$\int_{C_K^1}\chi(x)d^*x \quad \text{and} \quad \int_{C_K^1}\chi^\vee(x)d^*x$$

are zero if χ is nontrivial on $\mathbf{I}_K^1$; hence E is likewise zero in this case. When $\chi=\mu|\cdot|^s$ is trivial on $\mathbf{I}_K^1$, we know that in fact $\chi=|\cdot|^{s'}$, where $s'=s-i\tau$, for some real τ, and in this case,

$$\begin{aligned} E &= \int_0^1 \left[\hat{f}(0)t^{s'-1}\operatorname{Vol}(C_K^1) - f(0)t^{s'}\operatorname{Vol}(C_K^1)\right]\frac{1}{t}dt \\ &= \operatorname{Vol}(C_K^1)\left[\frac{\hat{f}(0)}{s'-1} - \frac{f(0)}{s'}\right] . \end{aligned}$$

Since E is a rational function, we get the desired meromorphic continuation of $Z(f,\chi)$ to the whole s-plane. We have also shown incidentally that it is holomorphic everywhere if $\mu\neq|\cdot|^{-i\tau}$, and that when $\mu=|\cdot|^{-i\tau}$, its only poles are at $s=i\tau$ and $s=1+i\tau$, with respective residues $-\operatorname{Vol}(C_K^1)f(0)$ and $\operatorname{Vol}(C_K^1)\hat{f}(0)$.

Finally, observe from Eqs. 7.8 and 7.9 that in fact the global zeta function may be expressed as

$$Z(f,\chi)=\int_1^\infty Z_t(f,\chi)\frac{1}{t}dt+\int_1^\infty Z_t(\hat{f},\chi^\vee)\frac{1}{t}dt+E(f,\chi)$$
$$=\int_1^\infty\int_{\mathbf{I}_K} f(tx)\chi(tx)\,d^*x\frac{1}{t}dt+\int_1^\infty\int_{\mathbf{I}_K}\hat{f}(tx)\chi^\vee(tx)\,d^*x\,\frac{1}{t}dt+E(f,\chi).$$

Moreover, since

$$\hat{\hat{f}}(x)=f(-x)\quad\text{and}\quad((\chi)^\vee)^\vee=\chi$$

it follows also that

$$Z(\hat{f},\chi^\vee)=\int_1^\infty Z_t(\hat{f},\chi^\vee)\frac{1}{t}dt+\int_1^\infty Z_t(\hat{\hat{f}},\chi)\frac{1}{t}dt+E(\hat{f},\chi^\vee)$$
$$=\int_1^\infty\int_{\mathbf{I}_K}\hat{f}(tx)\chi^\vee(tx)\,d^*x\frac{1}{t}dt+\int_1^\infty\int_{\mathbf{I}_K} f(-tx)\chi(tx)\,d^*x\,\frac{1}{t}dt+E(\hat{f},\chi^\vee).$$

But from our explicit formula above we see at once that E is invariant under the transformation $(f,\chi)\mapsto(\hat{f},\chi^\vee)$, and we may replace $\chi(tx)$ by $\chi(-tx)$ everywhere because χ is an idele-class character and hence indifferent to sign. Thus for K a number field we obtain the functional equation

$$Z(f,\chi)=Z(\hat{f},\chi^\vee)$$

as claimed.

The function field case remains. Here, by a similar argument, we get that

$$Z(f,\chi)=Z_1(f,\chi)+\sum_{n>0}Z_{t_n}(f,\chi)+\sum_{n>0}Z_{t_n}(\hat{f},\chi^\vee)+E'$$

where $\{t_n\}$ is a set of representatives of $\mathbf{I}_K$ modulo $\mathbf{I}_K^1$ with $|t_n|=q^n$, and

$$E'=\sum_{n<0}\left[\hat{f}(0)\chi^\vee(t_{-n})\int_{C_K^1}\chi^\vee(x)\,d^*x-f(0)\chi(t_n)\int_{C_K^1}\chi(x)\,d^*x\right].$$

Using the preceding proposition in the case $n=0$, we can write

$$Z_1(f,\chi)=\frac{1}{2}[Z_1(f,\chi)+Z_1(\hat{f},\chi^\vee)]+\frac{\hat{f}(0)}{2}\int_{C_K^1}\chi^\vee(x)d^*x-\frac{f(0)}{2}\int_{C_K^1}\chi(x)d^*x\ .$$

Putting $\varepsilon_n=1/2$ for $n=0$ or $\varepsilon_n=1$ if $n\geq 1$, we then find that

$$Z(f,\chi)=\sum_{n\geq 0}\varepsilon_n[Z_{t_n}(f,\chi)+Z_{t_n}(\hat{f},\chi^\vee)]\ +E$$

where

$$E=\begin{cases}0 & \text{if } \chi\neq|\cdot|^s\\ \sum_{n\geq 0}\varepsilon_n\operatorname{Vol}(C_K^1)[\hat{f}(0)q^{n(1-s)}-f(0)q^{-ns}] & \text{if } \chi=|\cdot|^s\ .\end{cases}$$

But $\sum_{n\geq 0}q^{nu}=1/(1-q^u)$, so when $\chi=|\cdot|^s$ we have that

$$E\ =\operatorname{Vol}(C_K^1)\cdot\left[\frac{\hat{f}(0)}{1-q^{1-s}}-\frac{f(0)}{1-q^{-s}}-\frac{\hat{f}(0)-f(0)}{2}\right].$$

The assertions of the theorem now follow as in the number field case. ❑

7.4 Hecke L-Functions

In this section we introduce and analyze global L-functions. While we state and prove the results only for number fields, even stronger results hold for function fields. In particular, in positive characteristic these L-functions turn out to be rational functions in q^{-s}, where q is the order of the corresponding field of constants. (See Exercise 22 below.)

Let χ be an idele class character of $\mathbf{I}_K$ for a number field K. As previously, we may write χ as $\mu|\cdot|^s$, where μ is unitary and $s\in\mathbf{C}$. Again, σ, the real part s, is called the exponent of χ. At each place v of K, we define a local character

$$\begin{aligned}\chi_v\colon K_v^* &\to \mathbf{C}^*\\ t &\mapsto \chi(1,\ldots,1,\underset{\substack{\uparrow\\ v\text{th component}}}{t},1,\ldots,1)\ .\end{aligned}$$

Then $\chi(y)=\prod_v\chi_v(y)$. Note that this makes sense because the restriction of χ_v is trivial on the units of $\mathfrak{o}_v$ for almost all v. (See Lemma 5-2.) Recall from Section 7.1 that we define the local L-factors at finite places v by

$$L(\chi_v) = \begin{cases} (1-\chi_v(\pi_v))^{-1} & \text{if } \chi_v \text{ is unramified} \\ 1 & \text{if } \chi_v \text{ is ramified.} \end{cases}$$

We may now define the (global) *L-function* of χ in terms of its local versions by the product expansion

$$L(\chi) = \prod_v L(\chi_v)$$

wherever this is convergent.

7-18 LEMMA. *$L(\chi)$ is absolutely convergent and nonzero whenever the exponent of χ is greater than* 1.

PROOF. Write χ as $\chi_0|\cdot|^s$, with σ=Re(s). With respect to convergence issues, we may ignore the finite set of places v where χ_v is ramified: since χ_v is trivial on the units of $\mathfrak{o}_v$ for almost all v, it is likewise unramified for almost all v. Then

$$\prod_v |L(\chi_v)| = \prod_v \frac{1}{|1-\chi_{0,v}(\pi_v)q_v^{-s}|}$$

and we must show that its logarithm converges for $\sigma>1$. Since

$$\log(\prod_v |L(\chi_v)|) = \sum_v \log(\frac{1}{|1-\chi_{0,v}(\pi_v)q_v^{-s}|})$$
$$= \mathrm{Re}(\sum_v \sum_{m>0} \frac{\chi_{0,v}(\pi_v)^m q_v^{-ms}}{m})$$

it suffices to establish the convergence of

$$\Sigma = \sum_v \sum_{m>0} \frac{q_v^{-m\sigma}}{m} .$$

We will do this for the number field case, leaving the function field case for an exercise. Letting p vary over the set of positive rational primes, write

$$\Sigma = \sum_p \sum_{v|p} \sum_{m>0} \frac{q_v^{-m\sigma}}{m} .$$

The number of v lying over any given prime p is bounded by $n=[K:\mathbf{Q}]$, and for each such v, the number q_v is a positive integral power of p. Therefore,

$$\Sigma \leq n\sum_p \sum_{m>0} \frac{p^{-m\sigma}}{m} = n\log(\prod_p \frac{1}{1-p^{-\sigma}}) .$$

But $\prod_p (1-p^t)$ is the classical Euler product, which sums to $\Sigma_{n\geq 1} n^{-t}$ and is absolutely convergent if $t>1$. ❑

DEFINITION. Let χ be an idele class character of $\mathbf{I}_K$. Then for complex s define the *Hecke L-function* $L(s,\chi)$ by

$$L(s,\chi) = L(\chi|\cdot|^s) .$$

It is also convenient to define finite and infinite versions of the Hecke L-function:

$$L(s,\chi_f) = \prod_{v \text{ finite}} L(s,\chi_v)$$

$$L(s,\chi_\infty) = \prod_{v \text{ infinite}} L(s,\chi_v)$$

The product of these two clearly gives $L(s,\chi)$. Note, in particular, that when $\chi=1$, we have

$$L(s,1_f) = \prod_{v \text{ finite}} \frac{1}{1-N(P_v)^{-s}}$$

where P_v is the prime associated with the finite place v and N is the absolute norm map. In particular, if $K=\mathbf{Q}$, we obtain the *Riemann zeta function*

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}} = \sum_{n\geq 1} \frac{1}{n^s}$$

in $\{\mathrm{Re}(s)>1\}$. For arbitrary K, $L(s, 1_f)$ is called the *Dedekind zeta function* of K, and denoted $\zeta_K(s)$. Just as in the rational case, for $\mathrm{Re}(s)>1$ we have

$$\zeta_K(s) = \sum_{\mathfrak{a}\neq 0} \frac{1}{N(\mathfrak{a})^s}$$

where $\mathfrak{a}$ runs over the set of nonzero ideals of $\mathfrak{o}_K$.

REMARKS. (i) Hecke actually considered a slightly different definition involving a generalized ideal class character; we explore this subsequently in Exercise 13. (ii) What we here denote $L(s,\chi)$ is sometimes written as $\Lambda(s,\chi)$; the notation $L(s,\chi)$ classically denotes that which we have called $L(s,\chi_f)$.

7-19 THEOREM. *Let χ be a unitary idele class character. Then $L(s,\chi)$, which is a priori defined and holomorphic in* $\{\mathrm{Re}(s)>1\}$, *admits a meromorphic continuation to the whole s-plane, and satisfies the functional equation*

$$L(1-s,\chi^\vee)=\varepsilon(s,\chi)L(s,\chi)$$

where

$$\varepsilon(s,\chi)=\prod_v \varepsilon(\chi_v|\cdot|^s)\in\mathbf{C}^*\ .$$

Moreover, this meromorphic continuation is entire unless $\chi=|\cdot|^{-i\tau}$, $\tau\in\mathbf{R}$, in which case there exist poles at $s=i\tau$ and $s=1+i\tau$, with respective residues $-\mathrm{Vol}(C_K^1)$ *and* $|N(\mathcal{D}_K)|^{-1/2}\,\mathrm{Vol}(C_K^1)$.

PROOF. First we claim that the asserted functional equation of $L(s,\chi)$ will follow once we show that it is meromorphic everywhere. Indeed, if we choose a factorizable $f=\otimes_v f_v\in S(\mathbf{A}_K)$, we will have (by Section 5.1) that with respect to any adele class character on $\mathbf{A}_K$,

$$Z(\hat{f},\chi^\vee)=\prod_v Z(\hat{f}_v,\chi_v^\vee)\ .$$

Specializing to the standard character ψ_K and appealing to the global functional equation of Section 7.3 and the local one of Section 7.1, we obtain

$$1=\prod_v\frac{\varepsilon(s,\chi_v)L(1-s,\chi_v^\vee)}{L(s,\chi_v)}=\frac{\varepsilon(s,\chi)L(1-s,\chi^\vee)}{L(s,\chi)}\ .$$

Hence we shall have our functional equation and meromorphic continuation, provided that $L(s,\chi)$ is indeed meromorphic.

That $L(s,\chi)$ is meromorphic in turn follows at once from Theorem 7-16 if we can establish the existence of a function $f=\otimes_v f_v\in S(\mathbf{A}_K)$ with the property that

$$Z(f,\chi|\cdot|^s)=h(s,\chi)L(s,\chi) \tag{7.10}$$

for a nonzero meromorphic function h. But we can see now that for every place v, we have already, in the proof of Theorem 7-2, constructed a local function $f_v\in S(K_v)$ such that

$$Z(f_v, \chi_v|\cdot|_v^s) = h_v(s,\chi_v)L(s,\chi_v)$$

where h_v is entire and everywhere nonzero for all v and, in fact, equal to 1 for almost all v. Indeed, in the real and complex cases the given Schwartz-Bruhat functions f_v yield $Z(f_v,\chi_v|\cdot|^s)=L(s,\chi)$ precisely. In the p-adic case, the local standard characters are given by

$$\psi_v(x) = \psi_p(\mathrm{tr}(x))$$

where v lies above the rational prime p. If we again let m_v denote the exponent of the conductor of ψ_v, which is zero for almost all v, then our previous construction takes the form

$$f_v(x) = \begin{cases} \psi_v(x) & \text{if } x \in P^{m_v - n_v} \\ 0 & \text{otherwise} \end{cases}$$

where n_v is the exponent of the conductor of χ_v. From our prior calculations (see Eqs. 7-4 and 7-5) and the normalization of d^*x_v to give volume $q^{m_v/2}$ on the local unit groups, it follows that

$$Z(f_v, \chi_v|\cdot|^s) = \begin{cases} q^{-m_v(s-1/2)}L(s,\chi_v) & \text{if } n_v = 0 \\ q^{-(m_v-n_v)s}g(\chi_v, \psi_{\pi_v^{m_v-n_v}})L(s,\chi_v) & \text{otherwise.} \end{cases}$$

Moreover, since n_v is zero for almost all v, we see that f_v is the characteristic function of $\mathfrak{o}_v$ for almost all v, and thus $f=\otimes_v f_v$ does indeed define a function f in $S(\mathbf{A}_K)$ such that $Z(f,\chi|\cdot|^s)$ has the requisite property of Eq. 7.10.

Finally, for $\chi=|\cdot|^{-i\tau}$ the expressions given for the residues are derived as follows from the corresponding residue formulas of Theorem 7-16. Locally we have everywhere that $f_v(0)=1$, which establishes the residue at $s=0$. To compute the residue at $s=1$, we can, via the global functional equation, simply compute the residue at $s=0$ for the Fourier transform of f_v. But in this case, $n_v=0$ for all v, so by construction f_v is the characteristic function of P^{m_v}, because this is precisely the conductor of ψ_v. It then follows from Exercise 7 below that

$$\hat{f}_v(0) = |N(\mathcal{D}_v)|^{-1/2} .$$

Thus taking the product of these over all v completes the proof. ❑

7.5 The Volume of C_K^1 and the Regulator

Let K again be a global field. Since the residue of $\zeta_K(s)$ at $s=1$ involves the volume of $C_K^1 = \mathbf{I}_K^1 / K^*$, it is our next order of business to compute it. First recall the following definitions and results from Chapter 5.

For any finite set S of places of K, let us now define the S-ideles of K by

$$\mathbf{I}_{K,S} = \{x = (x_v) \in \mathbf{I}_K : |x_v|_v = 1, \forall v \notin S\}$$

with norm-one version given by

$$\mathbf{I}_{K,S}^1 = \mathbf{I}_K^1 \cap \mathbf{I}_{K,S} .$$

Observe that here we do *not* require that S contain the infinite places of K, and thus this is a slight, but compatible, extension of the definition given previously in Chapter 5. Note also that $\mathbf{I}_{K,\varnothing} = \mathbf{I}_{K,\varnothing}^1$ is compact.

We shall prepare ourselves for the eventual volume calculation with three preliminary steps.

STEP ONE. Assume henceforth that S is nonempty. Then we have the short exact sequence

$$1 \to \mathbf{I}_{K,S}^1 \cdot K^* / K^* = \mathbf{I}_{K,S}^1 / K^* \cap \mathbf{I}_{K,S}^1 \to C_K^1 = \mathbf{I}_K^1 / K^* \to C_{K,S} = \mathbf{I}_K^1 / K^* \cdot \mathbf{I}_{K,S}^1 \to 1$$

where $C_{K,S}$ has finite order, say, h_S. (We proved this in Section 5.3 only for the case that S contains S_∞, but the present extension is trivial.) Consequently,

$$\mathrm{Vol}(C_K^1) = h_S \cdot \mathrm{Vol}(\mathbf{I}_{K,S}^1 / K^* \cap \mathbf{I}_{K,S}^1) \tag{7.11}$$

and our calculation is reduced to finding the volume of the second factor.

STEP TWO. Assume henceforth that K is a number field. Take $S=S_\infty$, the set of Archimedean places of K, and write Card(S) as the sum r_1+r_2, where r_1 is the number of real embeddings into a fixed algebraic closure of $\mathbf{Q}$, and r_2 is the number of nonconjugate complex embeddings. Define the *logarithmic map* as follows:

$$\lambda : \mathbf{I}_{K,S_\infty}^1 \to \mathbf{R}^{S_\infty} = \mathbf{R}^{r_1+r_2}$$
$$(x) \mapsto (\log|x_v|_v)_{v \in S_\infty} .$$

This is clearly a continuous homomorphism. Next define a hyperplane H in $\mathbf{R}^{r_1+r_2}$ by the equation

$$\sum_{v\text{ real}} t_v + 2\sum_{v\text{ complex}} t_v = 0 .$$

7-20 LEMMA. *The logarithmic map has the following properties:*

(i) $\mathrm{Im}(\lambda) = H$.

(ii) $\mathrm{Ker}(\lambda) = \mathbf{I}^1_{K,\varnothing}(=\mathbf{I}_{K,\varnothing})$.

PROOF. That the image of λ lies in H follows from two facts. First, that

$$\prod_{v\in S_\infty} |x_v|_v = 1 \quad \forall x = (x_v) \in \mathbf{I}^1_{K,S_\infty}$$

and second, that the normalized absolute value $|\cdot|_v$ coincides with the usual absolute value for v real and the square of the usual absolute value for v complex. Moreover, given $t=(t_v)\in H$, we can consider the idele $x=(x_v)$ with $x_v=1$ for v finite and $x_v\in K_v$ for $v\in S_\infty$ of ordinary absolute value t_v. Then by construction $\lambda(x)=t$, and this proves part (i). Since $|x_v|_v=1$ for all v for any $x\in\mathbf{I}_{K,\varnothing}$, it is obvious that $\mathbf{I}_{K,\varnothing}\subseteq\mathrm{Ker}(\lambda)$. Now suppose conversely that $x\in\mathbf{I}^1_{K,S_\infty}$ belongs to $\mathrm{Ker}(\lambda)$. Then $\log|x_v|_v=0$, i.e., $|x_v|_v=1$, for all $v\in S_\infty$. Thus $x\in\mathbf{I}^1_{K,\varnothing}(=\mathbf{I}_{K,\varnothing})$. ❑

The restriction of λ to $K^*\cap\mathbf{I}^1_{K,S_\infty}$ is called the *regulator map* and denoted $\mathrm{reg}(x)$. Recall that in fact,

$$\mathfrak{o}_K^\times = K^*\cap\mathbf{I}^1_{K,S_\infty} .$$

From the lemma above, we see that

$$\mathrm{Ker}(\mathrm{reg}) = \mathbf{I}^1_{K,\varnothing}\cap K^* = \mu_K$$

where μ_K is the set of roots of unity in K. Put

$$w_K = \mathrm{Card}(\mu_K) \quad\text{and}\quad L = \mathrm{reg}(\mathfrak{o}_K^\times) .$$

Then L is a discrete subgroup of H, which in turn is isomorphic to $\mathbf{R}^r$ where $r=r_1+r_2-1$. Also, since $\mathbf{I}^1_K/K^*$ is compact, H/L is likewise compact. Thus L is a full lattice in H.

STEP THREE. As our final preliminary for the calculation at hand, note that clearly, $\mathbf{I}^1_{K,\varnothing}$ admits the product decomposition

$$\prod_{v \text{ real}} U_v \times \prod_{v \text{ complex}} U_v \times \prod_{v \text{ finite}} U_v$$

where U_v denotes the subset of elements of K_v of absolute value one. We can thus establish a Haar measure on $\mathbf{I}^1_{K,\varnothing}$ given by the product measure whose factors are defined as follows:

- For v real, this is the counting measure on $U_v=\{\pm 1\}$.
- For v complex, this is the ordinary Lebesgue measure on S^1.
- For v finite, this is the normalized measure d^*x_v defined previously.

Thus

$$\mathrm{Vol}(U_v) = \begin{cases} 2 & \text{for } v \text{ real} \\ 2\pi & \text{for } v \text{ complex} \\ N(\mathcal{D}_v)^{-1/2} & \text{for } v \text{ finite} \end{cases}$$

where $\mathcal{D}_v$ is the different for finite v. Since one knows from Appendix B, Section 2, that the absolute value of the discriminant d_K (see also Chapter 4, Exercises 13 and 14) is given by

$$|d_K| = \prod_{v \text{ finite}} N(\mathcal{D}_v)$$

we get, relative to this measure,

$$\mathrm{Vol}(\mathbf{I}^1_{K,\varnothing}) = 2^{r_1}(2\pi)^{r_2}|d_K|^{-1/2} \;. \tag{7.12}$$

We may now combine the results of our three preliminary steps to obtain the following marvelous formula:

7-21 THEOREM. *Let K be a number field. Then we have*

$$-\mathrm{Res}_{s=1}\, \zeta_K(s) = \mathrm{Vol}(C_K^1) = \frac{2^{r_1}(2\pi)^{r_2} h_K R_K}{w_K\sqrt{|d_K|}}$$

where h_K is the class number of K and R_K is the regulator *of K; that is, the volume of H/L relative to the quotient measure induced by the map λ_* defined below.*

PROOF. From step two we have at once the commutative diagram below, all of whose rows and columns are exact:

$$
\begin{array}{ccccccccc}
 & & 1 & & 1 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mu_K & \to & \mathfrak{o}_K^\times & \xrightarrow{\text{reg}} & L & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mathbf{I}^1_{K,\varnothing} & \to & \mathbf{I}^1_{K,S_\infty} & \xrightarrow{\lambda} & H & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mathbf{I}^1_{K,\varnothing}/\mu_K & \to & \mathbf{I}^1_{K,S_\infty}/\mathfrak{o}_K^\times & \xrightarrow{\lambda_*} & H/L & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 0 & &
\end{array}
$$

The formula now follows at once from Eqs. 11 and 12. Note that R_K is computed with respect to the quotient measure induced (ultimately) by the measure on $\mathbf{I}^1_{K,\varnothing}$ established in step three and our standard measure on the idele group. ❑

REMARK. Let T $(=\mu_K)$ denote the torsion subgroup of $\mathfrak{o}_K^\times$, and define L' by

$$L' = (\mathfrak{o}_K^\times/T) \oplus \mathbf{Z}$$

which we regard as a free $\mathbf{Z}$-module. Define a homomorphism

$$\begin{aligned} \text{reg}' : L' &\to \mathbf{R}^{r_1+r_2} \\ (u,m) &\mapsto \text{reg}(u) + m\delta \end{aligned}$$

where $\delta=(\delta_v)_{v\in S_\infty}$ is the vector with $\delta_v=1$ (respectively, $\delta_v=2$) for v real (respectively, for v complex). Then it follows from the remarks above that reg$'$ is an embedding whose image is a full lattice in $\mathbf{R}^{r_1+r_2}$. This induces an isomorphism

$$(\text{reg}'\otimes\mathbf{R}) : L'\otimes\mathbf{R} \xrightarrow{\cong} \mathbf{R}^{r_1+r_2} .$$

One can check that R_K is none other than the absolute value of the determinant of this map relative to integral bases drawn from L' on the left and $\mathbf{Z}^{r_1+r_2}$ on the right. There are many situations in arithmetic and algebraic geometry where two lattices like this are sitting in a Euclidean space and the determinant of an

associated map from one to the other, as above, gives special values (or residues) of more general zeta functions. This is an active area of research.

We will conclude this section with the function-field case. Here we fix *any* place v_0 of K and take $S=\{v_0\}$. As previously, let $\mathrm{Div}^0(K)$ denote the group of divisors of degree zero on K; that is, finite formal sums D of the form

$$D=\sum_v n_v v \quad (n_v \in \mathbf{Z})$$

with $\deg(D) \doteq \sum_v n_v \deg(v)=0$. (See Section 7.2.) Again we have the *Picard group of degree zero* given by the quotient

$$\mathrm{Pic}^0(K) = \mathrm{Div}^0(K)/K^*$$

where each $f \in K^*$ defines the divisor $\mathrm{div}(f)=\sum_v v(f)v$. Recall that in forming this quotient, we are using implicitly that $\sum_v v(f)\deg(v)=0$, which is to say that f has as many zeros as poles, when counted with multiplicities. Indeed, this is true of any element x of adelic norm one because by definition, $\prod_v |x_v|_v=1$.

We may once again extend the divisor map from K^* to a larger structure:

$$\begin{aligned}\mathrm{div}: \mathbf{I}_{K,S}^1 &\to \mathrm{Div}^0(K)\\ x &\mapsto \sum_v v(x_v)v\ .\end{aligned}$$

Since x_v is a local unit at almost all v, we know that $v(x_v)$ is zero almost everywhere, and so the formal sum on the right has at most finitely many nonzero components. Moreover, arguing as above, $\sum_v v(f)\deg(v)=0$ because $x \in \mathbf{I}_{K,S}^1$, and thus the extended map is indeed well-defined. Finally, suppose that $x \in \mathrm{Ker}(\mathrm{div})$. Then $v(x_v)=0$ for all v, and therefore $x \in \mathbf{I}_{K,\varnothing}=\prod_v U_v$.

From the equality $\mathbf{I}_{K,\varnothing} \cap K^* = \mathbf{F}_q^*$, we get the short exact sequence

$$1 \to \mathbf{I}_{K,\varnothing}/\mathbf{F}_q^* \to \mathbf{I}_{K,S}^1/K^* \to \mathrm{Pic}^0(K) \to 0\ .$$

Thus $\mathrm{Pic}^0(K)$ is compact and discrete, and therefore finite. With these considerations in mind, we have the following function-field-theoretic version of our previous theorem:

7-22 THEOREM. *Let K be a function field over $\mathbf{F}_q$. Then*

$$-\mathrm{Res}_{s=1}\,\zeta_K(s) = \mathrm{Vol}(C_K^1) = \frac{1}{\log q}\cdot \mathrm{Card}(\mathrm{Pic}^0(K))\ . \qquad \square$$

7.6 Dirichlet's Class Number Formula

In this section, we shall specialize our results to the base field $\mathbf{Q}$, prove a factorization formula, and then recover the class number formula of Dirichlet for cyclotomic fields.

Recall from Section 6.5 that there is a natural identification of idele class characters χ of $\mathbf{Q}$ of finite order and the Dirichlet characters χ_D. By abuse of notation, we will write χ to denote either.

7-23 PROPOSITION. *Fix $m \geq 1$, and consider $F_m = \mathbf{Q}(e^{2\pi i/m})$. Then we have*

$$\zeta_{F_m}(s) = \prod_{\chi} L(s,\chi) \tag{7.13}$$

where the product runs over all the Dirichlet characters χ of conductor m_χ dividing m.

PROOF. It suffices to show that for each rational prime p the corresponding local factors are the same. In other words, we have to show that for $t=p^{-s}$,

$$\prod_{v|p}(1-t^{f_v}) = \prod_{\chi}(1-\chi(p)t) \tag{7.14}$$

where $f_v = [F_{m,v}:\mathbf{Q}_p]$. Since F_m is Galois over $\mathbf{Q}$, $f_v = f$ is the same for each of the g places v lying above p, and likewise, the corresponding ramification indices have a common value, which we denote e. We know further that

$$\varphi(m) = [F_m:\mathbf{Q}] = efg\ .$$

Hence the left-hand side of Eq. 7.14 may be rewritten and factored as follows:

$$\prod_{v|p}(1-t^{f_v}) = (1-t^f)^g = \prod_{z^f=1}(1-zt)^g\ .$$

Accordingly, one may obtain Eq. 7.14 at once from the following lemma, the proof of which we leave as an exercise.

7-24 LEMMA. *For every fth root of unity z there are g characters χ (mod m) such that $\chi(p)=z$.* ❑

Note that on the right side of Eq. 7.13, the factor corresponding to the trivial character is precisely the Riemann zeta function, which has a simple pole of

residue 1 at $s=1$. Thus by the residue computation of $\zeta_{F_m}(s)$ at $s=1$, we have the following formula:

$$\frac{(2\pi)^{\varphi(m)/2}}{w_m\sqrt{|d_m|}}h_mR_m = \prod_{\substack{\chi \bmod m \\ \chi\neq 1}} L(1,\chi) \ . \tag{7.15}$$

Here the symbols w_m, d_m, h_m, and R_m denote, respectively, the number of roots of unity, discriminant, class number, and regulator associated with F_m.

One can do better. Suppose that K is any finite abelian extension of $\mathbf{Q}$. By the Kronecker-Weber theorem, K is a subfield of some F_m. Put $G=\mathrm{Gal}(K/\mathbf{Q})$, which is a quotient group of $G_m=\mathrm{Gal}(F_m/\mathbf{Q})\cong(\mathbf{Z}/m\mathbf{Z})^\times$. Then its Pontryagin dual $\hat{G}$ is a subgroup of $\hat{G}_m$. Dirichlet characters χ modulo m are naturally identifiable with elements of $\hat{G}_m$. A refinement of the proof of Eq. 7.13 gives in this case the factorization

$$\zeta_K(s) = \prod_{\chi\in\hat{G}} L(s,\chi) \ .$$

In particular, $\zeta_K(s)$ is a factor of $\zeta_{F_m}(s)$. Now using the residue formula for $\zeta_K(s)$ at $s=1$, we obtain the following powerful theorem.

7-25 THEOREM. (Class Number Formula) *Let K be a finite abelian extension of $\mathbf{Q}$ with Galois group G, number of roots of unity w_K, class number h_K, regulator R_K, and discriminant d_K.* Let $r_1(K)$ and $r_2(K)$ *denote, respectively, the number of real and nonconjugate complex embeddings of K into an algebraic closure of $\mathbf{Q}$. Then we have*

$$\frac{2^{r_1(K)}(2\pi)^{r_2(K)}}{w_K\sqrt{|d_K|}}h_KR_K = \prod_{\substack{\chi\in\hat{G} \\ \chi\neq 1}} L(1,\chi) . \qquad \square$$

One may wonder at the importance of this formula. The reason is that $L(1,\chi)$ admits a concrete expression. Indeed, as we shall see in Exercise 14 below, by elementary Fourier analysis one may obtain an explicit formula:

7-26 PROPOSITION. *Fix $m\geq 1$, and let χ be a Dirichlet character modulo m. Then*

$$L(1,\chi) = \frac{-g(\chi)}{m}\sum_{a \bmod m}\bar{\chi}(a)\log(1-e^{-2\pi i a/m})$$

where $g(\chi)$ is the Gauss sum

$$\sum_{a \bmod m} \chi(a) e^{2\pi i a/m} .$$

More explicitly, we have

$$L(1,\chi) = \begin{cases} \dfrac{g(\chi)}{m^2} \pi i \displaystyle\sum_{a \bmod m} \bar{\chi}(a) a & \text{if } \chi(-1) = -1 \\ \dfrac{-g(\chi)}{m} \displaystyle\sum_{a \bmod m} \bar{\chi}(a) \log|1 - e^{2\pi i a/m}| & \text{if } \chi(-1) = +1 . \end{cases}$$ ❑

When this proposition is combined with the preceding theorem and then specialized to quadratic fields, we get the following beautiful result of Dirichlet.

7-27 THEOREM. (Dirichlet) *Let $K=\mathbf{Q}(\delta)$ be a quadratic field of discriminant $\delta^2=D$, and let χ_D be the quadratic Dirichlet character associated to K by class field theory; that is, for all rational primes p not dividing D, p splits in K if and only if $\chi_D(p)=1$. Then the root number for χ_D is given by*

$$W(\chi_D) = \frac{g(\chi_D)}{\sqrt{|D|}}(-1)^r \in \{-1,+1\}$$

where $r=0$ (respectively, 1) if $\chi(-1)=1$ (respectively, -1). Moreover:

(i) *If $D<0$, then*

$$h_K = -\frac{W(\chi_D) w_K i}{2D} \sum_{\substack{a \bmod D \\ (a,D)=1}} \bar{\chi}(a) a .$$

(ii) *If $D>0$, let u_0 denote the fundamental unit of K; that is, a generator of $\mathfrak{o}_K^\times$ modulo its torsion subgroup. Further let $u_c = u_0^{h_K}$. Then*

$$|u_c| = \prod_{\substack{0<a<D/2 \\ (a,D)=1}} |1 - e^{2\pi i a/D}|^{W(\chi_D)} .$$

PROOF. The assertion about $W(\chi_D)$ is developed in Exercise 15 below. Let $D<0$. Then $r_2=1$, $r_1=0$, $R_K=1$ (since $\mathfrak{o}_K$ has rank $r_1+r_2-1=0$), and $\hat{G}$ has a unique nontrivial character, which one can show to be χ_D. Also, K is imaginary if and only if $\chi_D(-1)=-1$, which says that the real prime does not split in K. It is easy

to check that the conductor m of χ_D is just $|D|$. This gives (i) immediately. When $D>0$, we have $r_1=2$, $r_2=0$, $w_K=2$, and $R_K=\log|u_0|$. Accordingly,

$$h_K \log|u_0| = \frac{-g(\chi)}{2\sqrt{D}} \cdot \sum_{\substack{a \bmod D \\ (a,D)=1}} \bar{\chi}(a)\log|1-e^{2\pi ia/D}| \, .$$

The asserted identity then follows by exponentiation, once we note that

$$\chi(a) = \chi(-a) \quad \text{and} \quad |1-e^{2\pi ia/D}| = |1-e^{-2\pi ia/D}| \, .$$

This completes the proof. ❑

7.7 Nonvanishing on the Line Re(s)=1

One of the consequences of Dirichlet's class number formula is that $L(1,\chi)$ is nonzero for any nontrivial Dirichlet character χ. The goal of this section is to prove, more generally, the following theorem.

7-28 THEOREM. *Let K be a number field and χ a unitary character of C_K. Then $L(s,\chi)$ does not vanish at $s=1+it$ for any $t\in\mathbf{R}$.*

PROOF. For χ unitary and $t\in\mathbf{R}$, note that $L(s,\chi|\cdot|^{it}) = L(s+it,\chi)$ and that $\chi|\cdot|^{it}$ is also unitary. Thus, after replacing χ by $\chi|\cdot|^{it}$, we may reduce the proof to showing that $L(s,\chi)$ has no zero at $s=1$ for any unitary character χ. Recall that $L(s,\chi)$ has a pole at $s=1$ if and only if $\chi=1$, in which case the pole is simple. Thus we may assume that χ is a nontrivial unitary character, and, since $L(s,\chi_\infty)$ has no zeros, show that

$$L(1,\chi_f) \neq 0 \, . \tag{7.16}$$

To do so, we shall separately treat two cases.

First consider the case that χ is quadratic; that is, $\chi^2=1$. (If $K=\mathbf{Q}$, this case is already known to us, but we shall give a unified treatment.) For Re(s)>1, define

$$L(s) = \zeta_K(s)L(s,\chi_f) \quad \text{and} \quad D(s) = \log L(s)$$

and continue $L(s)$ meromorphically to the whole s-plane via its factors. From the product expansions of $\zeta_K(s)$ and $L(s,\chi_f)$ we know that $L(s)$ has neither zero nor pole in {Re(s)>1}, and hence we may choose a single-valued branch of

$D(s)$ in that region. Moreover, from these same two expansions we see readily that

$$D(s)=\sum_{P\text{ prime}}\sum_{m\geq 1}\frac{1+\chi(P)^m}{N(P)^{ms}}\ . \tag{7.17}$$

This is a *Dirichlet series with nonnegative coefficients*, since $\chi(P)\in\{-1,0,+1\}$, and is absolutely convergent in $\{\mathrm{Re}(s)>1\}$.

Now we will give an argument based on a ubiquitous method of Landau, which requires two purely complex-analytic preliminaries.

7-29 LEMMA. *Let $D(s)=\sum_{n\geq 1}a_n/n^s$ and suppose that for some real number t, $D(s)$ converges absolutely at $s=t$. Then $D(s)$ converges normally in the region $\{\mathrm{Re}(s)>t\}$ and hence defines an analytic function there.*

PROOF. Replacing $D(s)$ by $D(s+t)$, we may assume that $t=0$. Then $\sum_{n\geq 1}a_n$ converges absolutely, and so for every $\varepsilon>0$ there exists a positive N such that

$$\sum_{n=N}^{k}|a_n|<\varepsilon$$

whenever $k\geq N$. It is easy to see (by regrouping terms) that

$$\sum_{n=N}^{k}|a_n|n^{-s}=\sum_{n=N}^{k-1}\Big(\sum_{r=N}^{n}|a_r|\Big)(n^{-s}-(n+1)^{-s})+\Big(\sum_{n=N}^{k}|a_n|\Big)k^{-s}$$

for any complex s, whence one immediately deduces that for real $\sigma>0$

$$\sum_{n=N}^{k}|a_n|n^{-\sigma}<\varepsilon\cdot\Big[\sum_{n=N}^{k-1}(n^{-\sigma}-(n+1)^{-\sigma})+k^{-\sigma}\Big]=\varepsilon N^{-\sigma}\leq\varepsilon\ .$$

This suffices to establish normal convergence in $\{\mathrm{Re}(s)>0\}$ because we can always shift the complex part of the exponential onto the a_n without disturbing the absolute convergence of the associated series. ❑

7-30 LEMMA. *Let $D(s)$ be as above and assume further that $a_n\geq 0$ for all $n\geq 1$. Suppose that $D(s)$ converges normally in $\{\mathrm{Re}(s)>t\}$ and that $D(s)$ is holomorphic at $s=t$. Then there exists a number $t_0<t$ such that the series $\sum_{n\geq 1}a_n/n^s$ converges in $\{\mathrm{Re}(s)>t_0\}$ and therefore represents $D(s)$ in this region.*

PROOF. Again, we may assume that $t=0$. Let $D(s)$ be holomorphic on a disk of radius R about zero, and choose $\delta<R/2$. Then for all positive σ we can write

$$D(\sigma) = \sum_{n\geq 1} a_n e^{-(\sigma-\delta)\log n} e^{-\delta \log n}$$

$$= \sum_{n\geq 1} a_n \left(\sum_{m\geq 0} \frac{(\delta-\sigma)^m (\log n)^m}{m!} \right) e^{-\delta \log n}$$

$$= \sum_{m\geq 0} \left(\sum_{n\geq 1} a_n (\log n)^m n^{-\delta} \right) \frac{(\delta-\sigma)^m}{m!} \ .$$

The rearrangement is valid because the nonnegativity of the a_n guarantees the requisite absolute convergence. (One may think of this as a discrete instance of Fubini's theorem.) This gives a power series expansion for $D(s)$ in a neighborhood of δ that must be valid in a disk of radius $R_1 > R/2$, since clearly such a disk can be inscribed in our original circle of radius R—within which $D(s)$ is holomorphic by assumption. Thus, reversing the force of the equality above, we find that the series representation $\sum_{n\geq 1} a_n/n^s$ is indeed valid to the right of zero, as asserted. ❑

Let us now return to the proof of the theorem. Restricting our attention to the real half-line, we have from Eq. 7.17 that $D(\sigma)$ takes on nonnegative real values for $\sigma > 1$. Suppose that $L(1,\chi_f) = 0$. Then we claim that $L(s)$ is invertible at $s=1$. Otherwise, it has a pole or a zero there. The former is impossible because $\zeta_K(s)$ has only a simple pole at $s=1$, and the latter is impossible because $D(\sigma)$ is nonnegative to the right of $s=1$, and therefore

$$\lim_{\sigma\to 1^+} D(\sigma) \neq -\infty \ .$$

Accordingly, we can continue $D(s)$ to the left until we encounter the first singularity, say at $\sigma_0 \in \mathbf{R}$, if indeed there is one. Applying the lemmas, we find that the expansion given by Eq. 7.17 is still valid for $\sigma_0 < \sigma$, which therefore remains nonnegative to the right of σ_0. This tells us that

$$\lim_{\sigma\to \sigma_0^+} D(\sigma) = +\infty \ .$$

But then $L(s)$ must have a pole (and not a zero) at $s=\sigma_0$. This is impossible because neither $\zeta_K(s)$ nor $L(s,\chi_f)$ has a pole at any point other than $s=1$ (and only in the former case). This means that we can continue $D(s)$ to the left as far as we want, say to $\sigma=-2$, and the previous expansion remains valid, with $D(\sigma)$ nonnegative on the real half-line. Now observe that $\zeta_K(s)$ has a zero at $s=-2$, because $\Gamma(s/2)^{r_1(K)}\Gamma(s)^{r_2(K)}\zeta_K(s)$ has no pole there, while $\Gamma(s)$ has simple poles at the values $s=0,-1,-2,\ldots$. [See Theorem 7-19 and the local constructions of the $L(\chi)$.] Since $L(s,\chi_f)$ has no pole, $L(s)$ has a zero at $s=-2$, whence it follows that

$$\lim_{\sigma \to -2} D(\sigma) = -\infty$$

—a contradiction! Therefore, $L(s,\chi_f) \neq 0$, as required.

Now let χ be nonquadratic. We set

$$L(s) = \zeta_K(s)^2 L(s,\chi_f) L(s,\overline{\chi}_f) \quad \text{and} \quad D(s) = \log L(s) .$$

Then

$$D(s) = \sum_P \sum_{m \geq 1} \frac{2 + \chi(P) + \overline{\chi}(P)}{N(P)^{ms}} .$$

Since χ is unitary, $\chi(P)$ is of the form e^{it_P}, and hence

$$2 + \chi(P) + \overline{\chi}(P) = 2 + 2\cos(t_P) \geq 0 .$$

Now the argument from the quadratic case goes through verbatim. ❑

The following result will be used in the next section.

7-31 PROPOSITION. *Let χ be a unitary idele class character of K. Then we have*

(i) *The summation*

$$\sum_{P \text{ prime}} \frac{\chi(P)}{N(P)^s}$$

is holomorphic at $s=1$, provided that χ is nontrivial.

(ii) *Moreover,*

$$\lim_{s \to 1^+} \sum_{P \text{ prime}} \frac{1}{N(P)^s} \Big/ \log\left(\frac{1}{s-1}\right) = 1 .$$

PROOF. Recall that $\log L(s,\chi)$ is absolutely convergent in $\text{Re}(s) > 1$, and note, moreover, that it equals

$$\sum_{P \text{ prime}} \frac{\chi(P)}{N(P)^s} + \sum_{m \geq 2} \sum_{P \text{ prime}} \frac{\chi(P)^m}{N(P)^{ms}} .$$

Now, on the one hand, the second series is dominated in absolute value by

$$\sum_{m\geq 2}\sum_{P \text{ prime}} \frac{1}{N(P)^{ms}}$$

which converges at $s=1$. On the other hand, if $\chi\neq 1$, $L(s,\chi)$ is invertible at $s=1$ by the previous theorem. Hence both

$$L(s,\chi) \quad \text{and} \quad \sum_{P \text{ prime}} \frac{\chi(P)}{N(P)^s}$$

are holomorphic at $s=1$. Now let $\chi=1$. Then $L(s,\chi)=\zeta_K(s)L(s,\chi_\infty)$ has a simple pole at $s=1$, and so we can write $\zeta_K(s)=(s-1)^{-1}H(s)$, with $H(s)$ invertible in $\{\text{Re}(s)\geq 1\}$. Then

$$\log\zeta_K(s) = \log(\frac{1}{s-1}) + \log H(s)$$

with $\log H(s)$ holomorphic at $s=1$. Thus

$$\lim_{s\to 1^+} (\sum_P \frac{1}{N(P)^s}) \Big/ \log(\frac{1}{s-1}) \;=\; \lim_{s\to 1^+} \frac{\log\zeta_K(s)}{\log(\frac{1}{s-1})} = 1$$

as claimed. ❑

Given any set S of primes P, we say that S has *Dirichlet*, or *analytic*, *density* $\delta=\delta(S)$ if we have

$$\lim_{s\to 1^+} (\sum_{P\in S} \frac{1}{N(P)^s}) \Big/ \log(\frac{1}{s-1}) = \delta \;.$$

It is part of the definition that the left-hand side converges; if it diverges, S has no Dirichlet density. Clearly $\delta(S)$ is unchanged if S is modified by a finite set, and, by the preceding proposition, $\delta(S)=1$ if S contains almost all the primes P in K. (See Exercise 16 below for further elaboration of these ideas.)

An immediate consequence of the proposition and some elementary Fourier analysis is the following celebrated theorem of Dirichlet on prime numbers in arithmetic progressions.

7-32 THEOREM. (Dirichlet) *Fix a positive integer m and let a be any integer relatively prime to m. Then there exist infinitely many rational primes p that are congruent to a modulo m. In fact, the set $S_{a,m}$ of such primes has Dirichlet density $1/\varphi(m)$.*

PROOF. Define

$$h(s) = \sum_{p \equiv a \bmod m} \frac{1}{p^s}.$$

Note that by the orthogonality of the characters of $(\mathbf{Z}/m\mathbf{Z})^\times$, given any integer b relatively prime to m, we have

$$\sum_{\chi \bmod m} \chi(b) = \begin{cases} \varphi(m) & \text{if } b \equiv 1 \bmod m \\ 0 & \text{otherwise.} \end{cases} \tag{7.18}$$

Accordingly, we may compute

$$g(s) \doteq \sum_{\chi \bmod m} \bar{\chi}(a)\Big(\sum_p \frac{\chi(p)}{p^s}\Big) = \sum_p \Big(\sum_{\chi \bmod m} \chi(a'p)\Big) p^{-s}$$

where a' is the multiplicative inverse of a modulo m. From Eq. 7.18 we see that

$$g(s) = \varphi(m) \cdot h(s).$$

By part (i) of the previous proposition,

$$\sum_p \frac{\chi(p)}{p^s}$$

is holomorphic at $s=1$ if χ is nontrivial. Thus

$$\lim_{s \to 1^+} h(s) / \log\Big(\frac{1}{s-1}\Big) = \frac{1}{\varphi(m)} \cdot \lim_{s \to 1^+} \frac{\sum_p \frac{1}{p^s}}{\log\big(\frac{1}{s-1}\big)} = \frac{1}{\varphi(m)}$$

by part (ii) of the same proposition. ❑

REMARK. Some number theorists prefer to work with "natural density" rather than the Dirichlet density. (See Section 6.2.) When the former exists for a set S of primes, then the latter exists as well, and the two densities are equal. But there are exotic S for which the latter exists, but not the former.

The Tchebotarev density theorem is a tremendous generalization of Dirichlet's theorem on primes in arithmetic progressions. Exercises 18–21 below will lead the reader through an elegant proof due to O. Schreier that uses the results

of this section. Also, Exercise 23 below will deal with the prime number theorem, or, more precisely, with its natural extension to arbitrary number fields.

7.8 Comparison of Hecke L-Functions

In this concluding section we shall prove the following beautiful theorem of Hecke, with an immediate and striking corollary. Throughout, K denotes an algebraic number field.

7-33 THEOREM. (Hecke) *Let μ_1 and μ_2 be unitary idele class characters of K. Suppose that the local components $\mu_{1,P}$ and $\mu_{2,P}$ are equal on a set $S=S(\mu_1,\mu_2)$ of primes of positive Dirichlet density. Then there exists a character χ of finite order on C_K such that $\mu_1=\chi\mu_2$. Moreover, for any $n\geq 1$, if $\delta(S)>1/n$, then χ has order less than n.*

7-34 COROLLARY. *If the Dirichlet density of S is greater than one-half, then in fact, $\mu_1=\mu_2$.* ❑

PROOF OF THEOREM. Let μ_1 and μ_2 be given as stated and suppose that $\delta(S)$ is positive. Suppose further that

$$\chi = \mu_1\mu_2^{-1}$$

is of order greater than or equal to some positive integer n. Then certainly $\chi^j\neq 1$ for all integers j of absolute value less than n. Define

$$D(s) = \sum_{P\text{ prime}} \frac{(\sum_{j=0}^{n-1}\chi^j(P))(\sum_{j=0}^{n-1}\chi^{-j}(P))}{N(P)^s}$$

and

$$D_S(s) = n^2\sum_{P\in S}\frac{1}{N(P)^s} .$$

Then both $D(s)$ and $D_S(s)$ are Dirichlet series with nonnegative coefficients. Moreover, since $\chi(P)=1$ for all $P\in S$, in fact, $D_S(s)$ is a subseries of $D(s)$, and both are absolutely convergent in $\text{Re}(s)>1$. For real $\sigma>1$, we can infer from the nonnegativity of the coefficients that

$$D_S(\sigma)\leq D(\sigma) . \tag{7.19}$$

CLAIM. *The function $D(s)$ has the following property:*

$$\lim_{\sigma\to 1^+} D(\sigma)/\log(\frac{1}{\sigma-1}) = n \ .$$

(It is here that we shall need to know that the order of χ is indeed greater than or equal to n.) Before proving the claim, let us see how it suffices to prove the theorem. Indeed, by definition we have that

$$\lim_{\sigma\to 1^+} D_S(\sigma)/\log(\frac{1}{\sigma-1}) = n^2\delta(S)$$

and by the inequality 7.19, this forces the inequality $\delta(S)\le 1/n$. But this will hold for every positive n if χ has infinite order, contrary to the hypothesis that $\delta(S)$ is positive. Thus χ must be of finite order, and if its order is greater than or equal to n, then $\delta(S)\le 1/n$. Thus the contrapositive holds, and this is precisely the assertion that if $\delta(S)>1/n$, then χ has order less than n. ❑

PROOF OF CLAIM. We first note that

$$D(s) = n\sum_P \frac{1}{N(P)^s} + \sum_{\substack{0\le j,k\le n-1\\ j\ne k}} \frac{\chi^{j-k}(P)}{N(P)^s} \ . \tag{7.20}$$

By the first part of Proposition 7-31, we have that the summation

$$\sum_P \frac{\nu(P)}{N(P)^s}$$

is holomorphic at $s=1$ for all characters $\nu\ne 1$, and this certainly applies to the characters χ^{j-k} for $0\le j,k\le n-1$, $j\ne k$, provided that the order of χ is at least n. Moreover, we know from the second part of that same proposition that

$$\lim_{s\to 1^+} (\sum_P \frac{1}{N(P)^s})/\log(\frac{1}{s-1}) = 1 \ .$$

The claim now follows directly from Eq. 7.20. ❑

REMARK. One can deduce this theorem from the stronger "equidistribution" result of Hecke on the values at Frobenius elements of any idele class character χ whose restriction to C_K° maps surjectively onto S^1. See Serre (1989, Appendix to Chapter 1) for a lovely treatment.

Exercises

1. Let F be a local field and let ψ be a nontrivial unitary character on F; that is, a continuous, nontrivial homomorphism from F as an additive group into S^1, the circle group. For each $a \in F$, define $\psi_a : F \to S^1$ by

$$\psi_a(x) = \psi(ax) .$$

(a) Show that ψ_a is again a unitary character of F, and that ψ_a is trivial if and only if $a = 0$.

(b) Show that $\psi \mapsto \psi_a$ defines a continuous, injective homomorphism α_ψ of F into its Pontryagin dual $\hat{F}$.

(c) Show that the image of α_ψ is dense in $\hat{F}$. [*Hint*: Show that $\psi_a(b) = 1$ for all $b \in F$ if and only if $b = 0$.]

(d) Show that α_ψ is bicontinuous.

(e) Show that $\alpha_\psi(F)$ is a complete, hence closed, subgroup of $\hat{F}$. Conclude that α_ψ is an isomorphism of topological groups.

2. Let F be a non-Archimedean local field with ring of integers $\mathfrak{o}_F$ and maximal ideal P. Fix a nontrivial unitary character ψ of F. Let P^m be the conductor of ψ; that is, the largest fractional ideal P^m on which ψ is trivial. Let α_ψ, as defined in the previous exercise, be the isomorphism between F and its Pontryagin dual.

(a) Show that via α_ψ, P^m identifies with the Pontryagin dual of $\hat{\mathfrak{o}}_F$. (This is also the inverse different of F, which soon makes its appearance.)

(b) Let $n \geq 1$ and $x \in F$. Show that $xP^n \in \mathrm{Ker}(\psi)$ if and only if $x \in P^{m-n}$.

3. In this exercise we construct nontrivial characters for non-Archimedean local fields, including the standard character for $\mathbf{Q}_p$ and its extensions, and the standard character for the completion of $\mathbf{F}_p(t)$ and its extensions, at the place defined by t^{-1}.

(a) Given any $x \in \mathbf{Q}_p$, let n be the smallest nonnegative integer such that $p^n x$ lies in $\mathbf{Z}_p$. Let r be such that $r \equiv p^n x \bmod p^n$. Put

$$\psi(x) = e^{2\pi i r/p^n} .$$

Show that $\psi:\mathbf{Q}_p \to S^1$ is a nontrivial unitary character of conductor $\mathbf{Z}_p$ and that it identifies with the composite map $\mathbf{Q}_p \to \mathbf{Q}_p/\mathbf{Z}_p \to \mathbf{Q}/\mathbf{Z} \to S^1$.

(b) Let K_∞ denote the completion of $K=\mathbf{F}_p(t)$ defined by the place t^{-1}. Show that $K_\infty=\mathbf{F}_p((t^{-1}))$; that is, that each $x \in K_\infty$ can be uniquely represented by a formal power series

$$\sum_{n=-\infty}^{r} a_n t^n$$

with $a_n \in \mathbf{Z}/p\mathbf{Z}$ for all n less than or equal to the integer r. Put

$$\psi_\infty(x) = e^{2\pi i a_1/p} \in S^1 \ .$$

Show that ψ_∞ is a nontrivial unitary character of K_∞ of conductor $\mathbf{F}_p[[t^{-1}]]$.

(c) Let π be any irreducible polynomial in $\mathbf{F}_p[t] \subseteq K$, and let K_π denote the completion of K defined by the prime ideal (π), with residue field k, which we may identify with a transversal of (π) in $\mathbf{F}_p[t]$. Show that every $x \in K_\pi$ can be written in the form

$$\sum_{n=r}^{+\infty} a_n \pi^n$$

for some integer r, with each coefficient $a_n \in k$. Next put

$$\psi_\pi(x) = e^{2\pi i \operatorname{tr}_{k/\mathbf{F}_p}(a_{-1})/p} \ .$$

Show that ψ_π is a nontrivial unitary character of K_π.

(d) Let F be any non-Archimedean local field. Show that F is a finite separable extension of a local field F_0 as in parts (a), (b), or (c) above. Let ψ_0 denote the corresponding character of F_0 defined therein. Given $x \in F$, set

$$\psi(x) = \psi_0(\operatorname{tr}_{F/F_0}(x)) \ .$$

Show that ψ is a nontrivial unitary character of F.

(e) Continuing in the same context, show that when the characteristic of F is zero, the conductor of ψ is the inverse different $\mathcal{D}_F^{-1}$. In this case show also that for f the characteristic function of $\mathfrak{o}_F$, the Fourier transform of f is $N(\mathcal{D}_F)^{-1/2}$ times the characteristic function of $\mathcal{D}_F^{-1}$.

4. We shall now construct the standard character on $\mathbf{A}_K/K$ for an algebraic number field K.

(a) For each rational prime p, let ψ_p denote the standard character of $\mathbf{Q}_p$ defined above. Also define $\psi_\infty:\mathbf{R}\to S^1$ by $\psi_\infty(x)=e^{-2\pi ix}$. Show that

$$\begin{aligned}\psi:\mathbf{A}_\mathbf{Q} &\to S^1\\ (x_v) &\mapsto \prod_v \psi_v(x_v)\end{aligned}$$

is a nontrivial unitary character on $\mathbf{A}_\mathbf{Q}$, which is trivial on $\mathbf{Q}$ (embedded diagonally). [*Hint*: Use the Artin product formula.]

(b) For any number field K, define $\psi_K:\mathbf{A}_K\to S^1$ by

$$\psi_K(x)=\prod_v \psi_v(x_v)$$

where v ranges over all the places of K and ψ_v is the standard character on the local field K_v, as constructed above. Show that ψ_K is a nontrivial unitary character on $\mathbf{A}_K$.

(c) Show also that $\psi_K(x)=\psi(\mathrm{tr}(x))$ where tr denotes the adelic trace map from K to $\mathbf{Q}$. Conclude from part (a) that ψ_K is trivial on K.

5. We shall now construct the standard character for the completion K_v of $K=\mathbf{F}_p(t)$ at any *finite* place v.

(a) Let $\pi(t)$ be an irreducible element of $\mathbf{F}_p[t]$ of degree $d\geq 1$. Show that K has a unique place v such that the polynomial $\pi(t)$ generates the maximal ideal $\mathfrak{o}_v=\{\alpha\in K_v:|\alpha|_v\leq 1\}$. Show further that $q_v=\mathrm{Card}(\mathfrak{o}_v/\pi\mathfrak{o}_v)=p^d$, and that the polynomials in $\mathbf{F}_p[t]$ of degree less than d in fact generate $\mathfrak{o}_v/\pi\mathfrak{o}_v$.

(b) Given any place v of K (possibly infinite), let us define

$$K^{(v)}=\{x\in K:|x|_u\leq 1\ \forall u\neq v\}\,.$$

Show that $K_v=K^{(v)}\oplus\mathfrak{o}_v$. [*Hint*: By replacing t by t^{-1} if necessary, one may assume that v is defined by an irreducible polynomial $\pi(t)\in\mathbf{F}_p[t]$ and then apply the previous part.]

(c) Let v be any finite place of K; that is, one defined by an irreducible polynomial $\pi(t)\in\mathbf{F}_p[t]$ of positive degree d. Show that every element y of $K^{(v)}$

can be written as z/π^n for some $n \geq 0$ and polynomial $z=z(t) \in \mathbf{F}_p[t]$ of the form

$$c_1 t^{nd-1} + c_2 t^{nd-2} + \cdots + c_{nd}$$

with $c_j \in \mathbf{F}_p$ for all j, possibly all zero. If $x = y + \alpha \in K_v$ with $\alpha \in \mathfrak{o}_v$, put

$$\psi_v(x) = e^{2\pi i c_1/p}.$$

(This is of course well-defined despite the status of c_1 as a residue class modulo the prime p.) Show that ψ_v is a nontrivial character of K_v of conductor $\mathfrak{o}_v$.

(d) Let v, π, and y be as in the previous part. Show that $y \equiv a_1 t^{-1} \pmod{t^{-2}}$. Conclude that $\psi_v(y)\psi_\infty(y)=1$, where ψ_∞ is as in part (b) of Exercise 3. [*Hint*: Write π as $t^d g$, with g a polynomial in t^{-1} of constant term 1, so that $y = fg^{-n}t^{-nd}$.]

6. We may now use the results of previous problems to construct the standard character $\psi_K : \mathbf{A}_K \to S^1$ for K any global field of positive characteristic.

(a) Suppose that $K_0 = \mathbf{F}_p(t)$. Define ψ_{K_0} by

$$\psi_{K_0}(x) = \prod_v \psi_v(x_v)$$

where ψ_∞ is given by Exercise 3 and ψ_v (v finite) is given by part (c) of the previous exercise. Show that ψ_{K_0} is a nontrivial character of $\mathbf{A}_{K_0}$ that moreover, is trivial on K_0.

(b) Now let K be any finite separable extension of K_0. Use the trace map from K to K_0 (or, equivalently, the corresponding adelic trace map) to define the standard character ψ_K on K. Show that this character is nontrivial on $\mathbf{A}_K$, but trivial on K.

7. Let G be a locally compact abelian group with Haar measure dg, and let $d\hat{g}$ be the dual measure; that is, the measure on the Pontryagin dual $\hat{G}$ relative to which the Fourier inversion formula holds. Suppose that we have an isomorphism $\alpha : G \xrightarrow{\cong} \hat{G}$ of topological groups.

(a) Show that there is a *unique* multiple $\mu = t \cdot dg$ such that μ identifies with its dual measure under α. One calls μ the *self-dual* measure on G relative to the isomorphism α.

(b) Let G be the additive group of a non-Archimedean local field F, $\psi: F \to S^1$ the standard unitary character, and α_ψ the isomorphism of Exercise 1. Denote by dx the self-dual measure relative to ψ (that is, relative to α_ψ). Show that $\mathrm{Vol}(\mathfrak{o}_F, dx) = N(\mathcal{D}_F)^{-1/2}$, where $\mathcal{D}_F$ denotes the different of F.

8. In this exercise we analyze the dependence of the epsilon factor on the additive character ψ and the Haar measure dx. Let F be a local field and consider $\varepsilon(\chi, \psi, dx)$ for any $\chi \in \mathrm{Hom}_{\mathrm{cont}}(F^*, \mathbf{C}^*)$.

(a) For every positive real number t, show that

$$\varepsilon(\chi, \psi, t \cdot dx) = t \cdot \varepsilon(\chi, \psi, dx) .$$

(b) Let $a \in F^*$, and let ψ_a denote the character defined by $\psi_a(x) = \psi(ax)$. Show that

$$\varepsilon(\chi, \psi_a, dx) = \chi(a)|a|^{-1} \varepsilon(\chi, \psi, dx) .$$

(c) Let F be non-Archimedean with unique prime ideal P, and let P^n and P^m be the conductors of χ and ψ, respectively. Then show for every unramified character ν of F^* that

$$\varepsilon(\chi\nu, \psi, dx) = \nu(\pi^{m+n}) \varepsilon(\chi, \psi, dx)$$

where π is a uniformizing parameter for $\mathfrak{o}_F$. Note that the first factor on the right is well-defined because ν is unramified. [*Hint*: Use the explicit formula given in Eq. 7.6.]

9. Let F be a local field with standard character ψ and self-dual measure dx, and let $\chi = \omega | \cdot |^s$ be a (quasi-) character on F^* with ω unitary. Put

$$W(\omega) = \varepsilon(\chi, \psi, dx)\big|_{s=\frac{1}{2}} .$$

(a) By using the functional equation, show that

$$W(\omega) W(\overline{\omega}) = \omega(-1) .$$

Conclude that $|W(\omega)| = 1$. [*Hint*: First prove that $W(\overline{\omega}) = \omega(-1)\overline{W(\omega)}$.]

(b) Using Section 7.1, show that for $F = \mathbf{R}$, $W(\omega) = 1$ (respectively, $-i$) for $\omega = 1$ (respectively, $\omega = \mathrm{sgn}$). Show further that when $F = \mathbf{C}$, we have $W(\omega) = 1$.

(c) Let F be non-Archimedean with uniformizing parameter π, and let ω as above have conductor $\pi^n\mathfrak{o}_F$. Put

$$G = \sum_{x\in U/U_n} \overline{\omega}(x)\psi(x\pi^{d-n})$$

where $\pi^d\mathfrak{o}_F = \mathcal{D}_F$ (the different), $U_r = 1+\pi^r\mathfrak{o}_F$ $(r>0)$, and U is the full group of units in $\mathfrak{o}_F$. Show directly that $|G|^2 = q^n$. Then appeal to Eq. 7.6 to deduce (once again) that $|W(\omega)|=1$.

10. (Tate) Let F be a non-Archimedean local field with uniformizing parameter π, and let ω be a unitary character of F^* with conductor $\pi^n\mathfrak{o}_F$. Let $\mathfrak{a}$ be an ideal of $\mathfrak{o}_F$ such that $\mathfrak{a}^2$ divides $\pi^n\mathfrak{o}_F$. Put $\mathfrak{b}=\mathfrak{a}^{-1}\pi^n\mathfrak{o}_F\subseteq\mathfrak{o}_F$.

(a) Show that there exists an element $c\in F$ such that $c\mathfrak{o}_F = \pi^n\mathcal{D}_F$ and also

$$\omega(1+t) = \psi(c^{-1}t)$$

for all $t\in\mathfrak{b}$. [*Hint*: Suppose that $\mathfrak{a}\neq\mathfrak{o}_F$, so that π divides $\mathfrak{a}$. If $t,z\in\mathfrak{b}$, then $tz\in\pi^n\mathfrak{o}_F$. Consequently, $\omega(1+t)\,\omega(1+z)=\omega(1+t+z)$, and therefore the map that sends t to $\omega(1+t)$ is a character of the additive group $\mathfrak{b}$, and this extends to one on F. Now appeal to the isomorphism of F with its dual.]

(b) For c as in the previous part and F now assumed to have characteristic zero, show that

$$W(\omega) = N(\mathfrak{b}\mathfrak{a}^{-1})^{-1/2} \sum_{x\in(1+\mathfrak{a})/(1+\mathfrak{b})} \overline{\omega}(c^{-1}x)\,\psi(c^{-1}x)\ .$$

NOTE. When $\mathfrak{a}=\mathfrak{o}_F$, this result is identical to Eq. 7.6.

(c) For ω unramified, show that $W(\omega)=\omega(\pi)^d$ if $\pi^d\mathfrak{o}_F=\mathcal{D}_F$.

(d) Let E be a number field containing $W(\omega)$. Then show that for every place v of E not dividing the residual characteristic p of F, we have $|W(\omega)|_p=1$. Using the Artin product formula, conclude that if E has a unique place u above p, then also $|W(\omega)|_u=1$.

(e) Suppose that $\pi^n\mathfrak{o}_F=\pi\mathfrak{a}$. Then, using part (b), show that $z=(\omega(c^{-1})\,W(\omega))^2$ lies in the cyclotomic extension $E=\mathbf{Q}(e^{2\pi i/p^r})$ for some $r\geq 1$. Show further, using part (d), that z must be a root of unity.

(f) (Lamprecht, Dwork) Suppose that ω is either *unramified* (that is, $n=0$) or *wildly ramified* (that is, $n\geq 2$). Show that $W(\omega)$ is a root of unity. [*Hint*: This is clear if n is even. When n is odd, write $\pi^n \mathfrak{o}_F = \pi\mathfrak{a}$ and apply the previous part.]

11. Let K be a global field. For any idele class character $\chi=(\chi_v)$, put

$$W(\chi)=\prod_v W(\chi_v) \ .$$

(a) Show that $W(\chi)\,W(\chi^{-1})=1$. In particular, if χ is unitary, then $|W(\chi)|=1$.

(b) Let K be a number field, and let χ be quadratic or trivial. Conclude from part (a) that $W(\chi)=\pm 1$. [This number is called the *sign of the functional equation* of $L(s,\chi)$.] Show, moreover, that if χ is unramified everywhere, then

$$W(\chi)=\tilde{\chi}(\mathcal{D}_K)$$

where $\tilde{\chi}$ is the associated character of the class group Cl_K (cf. Proposition 5-19). [*Hint*: Use the previous problem.]

(c) Let χ be a quadratic idele class character, and let E/K be the quadratic extension corresponding to the open subgroup $\mathrm{Ker}(\chi)$ of C_K by class field theory (Theorem 6-6). Note that $\zeta_E(s)=\zeta_K(s)\,L(s,\chi)$ and deduce the formula

$$\varepsilon(s,\chi)=(|d_K|/|d_E|^{1/2})^{1-2s}$$

where d_K and d_E are the discriminants of K and E, respectively.

(d) (Hecke's Theorem, Serre's Proof) Let K be a number field. Then prove:

THEOREM. (Hecke) *The ideal class of $\mathcal{D}_K$ is a square in the class group Cl_K.*

[*Hint*: Observe that it suffices to show that $\tilde{\chi}(\mathcal{D}_K)=1$ for every quadratic character $\tilde{\chi}$ of Cl_K. Then appeal to parts (b) and (c) of this problem.]

12. We consider here the Fourier transforms of Schwartz-Bruhat functions.

(a) Let F be a local field. Show that for every $f\in S(F)$, its Fourier transform likewise lies in $S(F)$. [*Hint*: For F Archimedean, this is a well-known classical fact. In the non-Archimedean case, use that f is a linear combination of

characteristic functions of the basic compact sets P^n, where P is the unique prime associated with F.)

(b) Let K be a global field and assume that $f \in S(\mathbf{A}_K)$. Show that the Fourier transform of f is likewise in $S(\mathbf{A}_K)$. [*Hint*: First prove that $S(\mathbf{A}_K)$ is generated by factorizable functions $\otimes_v f_v$, where each f_v lies in $S(K_v)$ for all v, and then use the previous part to establish the result in this special case.]

(c) Use the results of Chapter 3 to show that the Fourier transform map $S(\mathbf{A}_K) \to S(\mathbf{A}_K)$ extends to an isometry $L^2(\mathbf{A}_K) \to L^2(\mathbf{A}_K)$.

13. (Hecke Characters) Let K be a number field of degree d, let S be a finite set of places containing S_∞, and let $J_K(S)$ be the group of fractional ideals prime to S. Furthermore, let $\mathbf{I}_K(S)$ denote the subgroup of $\mathbf{I}_K$ consisting of ideles $y=(y_v)$ such that $y_v=1$ at every place v in S.

(a) Define $\alpha: \mathbf{I}_K(S) \to J_K(S)$ by

$$\alpha(y) = \prod_{v \notin S} P_v^{v(y_v)} .$$

Show that α is a surjective homomorphism with kernel

$$U(S) = \{y \in \mathbf{I}_K(S) : y_v \in \mathfrak{o}_v^\times , \forall v \text{ finite}\} .$$

Conclude that every character χ of $\mathbf{I}_K$ that is unramified outside S defines a character $\tilde{\chi}$ of $J_K(S)$.

(b) Let β be a *Grössencharakter* (or *Hecke character*) of K, which is to say a homomorphism from $J_K(S)$ to $\mathbf{C}^*$ for which there exists an integral ideal M with support S, complex numbers $s_1,\ldots,s_d$ and integers $m_1,\ldots,m_d$ such that for every $\alpha \in K^*(M)$, one has

$$\beta((\alpha)) = \prod_{j=1}^{d} \sigma_j(\alpha)^{m_j} |\sigma_j(\alpha)|^{s_j}$$

where $\{\sigma_j\}$ is the set of embeddings of K in $\mathbf{C}$. Show that every β is of the form $\tilde{\chi}$ for some character $\chi: \mathbf{I}_K \to \mathbf{C}^*$ that is trivial on K^*. [*Hint*: Show that β defines a character of the ray class group $Cl_K(M)$ and then lift it to the idele class group C_K.]

(c) Let $\Phi=\tilde{\chi}$ for an idele class character χ unramified outside S. Show that Φ is in fact a *Grössencharakter*. [*Hint*: Take

$$M=\prod_{v\in S} P_v^{\max(1,n_v)}$$

where n_v is the exponent of the conductor of χ_v. For $\alpha\in K^*(M)$, show that $\Phi((\alpha))=\Pi_{v\notin S}\chi_v(\alpha)=1/\chi_\infty\circ\sigma(\alpha)$ by using first that $|\alpha_v|_v=1$ for all v in S and second that χ is trivial on K^*.]

14. Fix an integer $k\geq 1$, and consider the *polylogarithm* function

$$l_k(z)=\sum_{n\geq 1}\frac{z^n}{n^k}\,.$$

Note that $l_1(z)=-\log(1-z)$. The special case of $l_2(z)$ is called *Euler's dilogarithm* function.

(a) Show that the series is normally convergent in the open unit disk $\{|z|<1\}$ and that it has finite limit on the unit circle S^1 (respectively, $S^1-\{1\}$) if $k>1$ (respectively, $k=1$).

(b) Let χ be a Dirichlet character of conductor $m\geq 1$. For w an mth root of unity, put

$$G(\chi,w)=\sum_{c \bmod m}\chi(c)w^c\,.$$

Let $L(s,\chi)$ be the Dirichlet L-series, and assume that χ is not the trivial character if $k=1$. Put $\chi(-1)=(-1)^r$. Then show that

$$L(k,\chi)=\frac{1}{m}\sum_{1\leq b\leq m/2}G(\chi,e^{-2\pi ib/m})[l_k(e^{2\pi ib/m})+(-1)^r l_k(e^{-2\pi ib/m})]$$

[*Hint*: Expand χ in terms of the basis $\{e^{2\pi ib/m}:0\leq b<m\}$ of $\mathbf{C}[\mathbf{Z}/m\mathbf{Z}]$.]

(c) Show that

$$G(\chi,e^{-2\pi ib/m})=\bar{\chi}(b)G(\chi,e^{-2\pi i/m})\,.$$

Simplify part (b) accordingly for $k=1$ and deduce Proposition 7-26.

(d) For any $k \geq 1$, show that there is an elementary expression for the Dirichlet series $L(k,\chi)$ if $\chi(-1)=(-1)^k$.

15. Let χ be a Dirichlet character of conductor $m \geq 1$. As above, put

$$W(\chi) = \varepsilon(\chi|\cdot|^{1/2}) \; (=\varepsilon(1/2,\chi)) \, .$$

Show that

$$W(\chi) = \frac{G(\chi)}{\sqrt{m}}(-i)^r$$

where $r=0$ (respectively, 1) if $\chi(-1)=1$ (respectively, -1), and

$$G(\chi) = \sum_{a \bmod m} \chi(a) e^{2\pi i a/m} \, .$$

16. Let K be a number field and let S be a set of primes in $\mathfrak{o}_K$. One says that S has *lower Dirichlet density*

$$\underline{\delta}(S) = \liminf_{s \to 1^+} \frac{1}{\log \frac{1}{s-1}} \cdot \sum_{P \in S} \frac{1}{N(P)^s}$$

provided that the indicated lim inf exists. The *upper Dirichlet density* $\overline{\delta}(S)$ is likewise defined via the lim sup.

(a) Show that every S has both a lower and an upper Dirichlet density. [*Hint*: Use Proposition 7-31, part (ii), and also that a bounded sequence in $\mathbf{R}$ has an infimum and a supremum.]

(b) Show that S has a Dirichlet density (as defined previously) if and only if $\underline{\delta}(S) = \overline{\delta}(S)$.

(c) Let T be any finite set of primes in $\mathfrak{o}_K$. Show that $\underline{\delta}(S \cup T) = \underline{\delta}(S)$ and $\overline{\delta}(S \cup T) = \overline{\delta}(S)$. Conclude, in particular, that any finite set of primes has density zero.

(d) Let $\mathscr{P}_K^1$ denote the set of degree-one primes of K; that is, prime ideals of $\mathfrak{o}_K$ such that $N(P)=1$. Show that for any set S of primes, $\underline{\delta}(S \cap \mathscr{P}_K^1) = \underline{\delta}(S)$ and $\overline{\delta}(S \cap \mathscr{P}_K^1) = \overline{\delta}(S)$. Conclude that the set of primes in $\mathfrak{o}_K$ of degree greater than one has density zero.

17. Let E/K be a finite abelian extension of number fields with Galois group $G=\mathrm{Gal}(E/K)$. Let $U=N_{E/K}(C_E)$. Recall that C_K/U is isomorphic to G via class field theory. (See Theorem 6-6.) For any character χ of G, let $\tilde{\chi}$ denote the corresponding character of C_K that is trivial on U. Keeping in mind that the extension E/K is abelian, for any prime P of K, we let

$$\varphi_P = \left(\frac{E/K}{P}\right)$$

denote the corresponding Frobenius element. Now set

$$\chi(P) = \begin{cases} \chi(\varphi_P) & \text{if } P \text{ is unramified in } E \text{ or if } \chi \text{ is trivial} \\ 0 & \text{otherwise} \end{cases}$$

and put

$$L(s,\chi) = \prod_P (1-\chi(P)N(P)^{-s})^{-1} .$$

(a) Show that $L(s,\chi)$ converges absolutely in $\{\mathrm{Re}(s)>1\}$ and further admits a meromorphic continuation to the whole s-plane, with no poles except possibly a simple one at $s=1$, which occurs only when $\chi=1$. Show, moreover, that there is a functional equation relating s to $1-s$. [*Hint*: Use Theorems 6-6 and 7-16.]

(b) Show that

$$\zeta_E(s) = \prod_{\chi\in\hat{G}} L(s,\chi) .$$

[*Hint*: Write the left-hand side as an Euler product over the primes P of K.]

(c) Show that

$$\lim_{x\to 1^+} \frac{1}{\log\frac{1}{s-1}} \sum_{P\in\mathscr{P}_K^1} \frac{\chi(P)}{N(P)^s} = \begin{cases} 1 & \text{if } \chi=1 \\ 0 & \text{otherwise.} \end{cases}$$

The following four problems lead the reader through a proof of a version of the Tchebotarev density theorem, here reformulated in terms of Dirichlet density. Recall that $\mathscr{P}_{Kf}$ denotes the set of finite places of K, or, equivalently, the set of prime ideals of $\mathfrak{o}_K$.

THEOREM. *Let E/K be a finite Galois extension of number fields with Galois group G, and let C be a conjugacy class in G. Set*

$$S_K(C)=\{\,P\in\mathscr{P}_{K,f}:\left(\frac{E/K}{P}\right)=C\,\}\,.$$

Then $\delta(S_K(C))$ *exists and equals* $\mathrm{Card}(C)/\mathrm{Card}(G)$.

We shall also need the degree-one version of $S_K(C)$, which we define as

$$S_K^1(C)=S_K(C)\cap\mathscr{P}_K^1\ .$$

The first problem is well known and deals with the abelian case. The next three encapsulate the ideas from an elegant proof due to O. Schreier.

18. Let E/K be a finite abelian extension, so that C reduces to a singleton set $\{a\}$ for some $a\in G$. We recall from Chapter 3, Exercise 13, the discrete form of the Fourier inversion formula: if f is a complex-valued function on G, then

$$f(g)=\frac{1}{\mathrm{Card}(G)}\sum_{\chi\in\hat{G}}\hat{f}(\chi)\chi(g)$$

where

$$\hat{f}(\chi)=\sum_{g\in G}f(g)\bar{\chi}(g)\,.$$

(a) Given $a\in G$, define $f_a\colon G\to\mathbf{C}$ by

$$f_a(g)=\sum_{\chi\in\hat{G}}\chi(a^{-1}g)\ .$$

Show that f_a is in fact the characteristic function of $\{a\}$.

(b) For all $g\in G$ show that

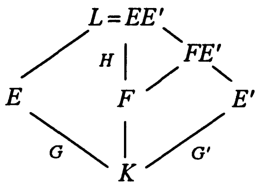
$$\sum_{P\in S_K(C)}\frac{1}{N(P)^s}=\sum_{g\in G}\sum_{P\in S_K(C)}\frac{f_a(g)}{N(P)^s}=\frac{1}{\mathrm{Card}(G)}\sum_{\chi\in\hat{G}}\sum_{P}\frac{\chi(P)}{N(P)^s}\ .$$

(c) Show that $\delta(S_K(C))$ exists and equals $1/\mathrm{Card}(G)=\mathrm{Card}(C)/\mathrm{Card}(G)$. [*Hint*: Use the previous exercise.]

19. Suppose that E/K is any finite normal extension of number fields. Let G be the associated Galois group, and let C be a conjugacy class in G. Suppose further that E' is an auxiliary finite abelian extension of K with Galois group G' such that E and E' are linearly disjoint over K. Put $L=EE'$.

(a) Show that L/K is normal with Galois group $\mathcal{G}=G\times G'$.

(b) Choose any conjugacy class $C'=\{a\}$ in G', and let H be the subgroup generated by CC' in $\mathcal{G}$. Put $F=L^H$, and consider the compositum FE'. We have the following diagram:



Show that FE' is a normal extension of F with Galois group given by

$$\mathrm{Gal}(FE'/F) \cong H/H\cap\langle C\rangle \cong \langle C'\rangle \subseteq G' .$$

Using the previous problem, conclude that

$$\delta(\{ Q \in \mathcal{P}_F^1 : \left(\frac{FE'/F}{Q}\right) = C' \}) = \frac{1}{f'}$$

where $f'=\mathrm{Card}(\langle C'\rangle)$.

(c) For $P \in S_K^1(C)$, define $\alpha_P(F)=\mathrm{Card}(\{ Q \in \mathcal{P}_F^1(C) : Q|P\})$. Show that

$$\alpha_P(F) = \frac{1}{\mathrm{Card}(H)}\mathrm{Card}(\{\tau \in \mathcal{G} : \tau C\tau^{-1} \in H\}) .$$

[*Hint*: Use Proposition 6-2.]

(d) Put $f=\mathrm{Card}(C)$. Assuming that $f\,|\,f'$, show for $P \in S_K^1(C)$ that

$$\left(\frac{L/K}{P}\right) \cap H = \varnothing .$$

20. We continue in the context of the previous problem and always assume that $f\,|\,f'$.

(a) Show that

$$\lim_{s\to 1^+} \sum_{P\in S_K^1(C,C')} \frac{\alpha_P(F)}{N(P)^s} \sim \frac{1}{f'}\log\left(\frac{1}{s-1}\right)$$

where

$$S_K^1(C,C') = \{P \in S_K^1(C) : \left(\frac{E'/K}{P}\right) = C'\}.$$

(b) Show that

$$\delta(S_K^1(C,C')) = \frac{f}{nn'}$$

where n and n' denote Card(G) and Card(G'), respectively. [*Hint*: Show that $\alpha_P(F)=nn'/ff'$.]

(c) Let

$$n'_f = \mathrm{Card}(\{\sigma' \in G' : f \mid o(\sigma')\}).$$

Show that

$$\underline{\delta}(S_K(C)) \geq \frac{fn'_f}{nn'}$$

where again $\underline{\delta}$ denotes lower Dirichlet density, as defined above. [*Hint*: Any absolutely convergent summation indexed over $P \in S_K^1(C)$ can be rewritten as a double summation, first over $\sigma' \in G'$ and then over

$$\{P \in S_K^1(C) : \left(\frac{E'/K}{P}\right) = \sigma'\}.$$

Use this and appeal to part (b).]

21. We continue in the context of the previous two problems.

(a) Show that we can choose G' such that the quotient n'_f/n is arbitrarily close to 1. [*Hint*: Suppose that f has prime factorization

$$f = \prod_{j=1}^{r} p_j^{a_j} \quad (a_j > 0) .$$

Then take G' of order

$$\prod_{j=1}^{r} p_j^{b_j}$$

such that for each j, $p_j^{b_j} - p_j^{a_j - 1}$ elements of G' have order a power of $p_j^{a_j}$.]

(b) Use the previous exercise and the first part of this one to show that

$$\underline{\delta}(S_K(C)) \geq \frac{f}{n} .$$

(c) Show that

$$\underline{\delta}(S_K(G-C)) \geq \frac{n-f}{n} .$$

[*Hint*: $G-C$ is the disjoint union of conjugacy classes different from C.]

(d) Show that $\delta(S_K(C))$ exists and is given by $f/n = \mathrm{Card}(C)/\mathrm{Card}(G)$. [*Hint*: Use part (c) to conclude that

$$\overline{\delta}(S_K(C)) \leq \frac{f}{n} .$$

But the lower and upper Dirichlet densities always exist, and the latter bounds the former from above.]

22. Let K be a function field in one variable over a finite field $\mathbf{F}_q$. The first parts of this exercise lead to a proof of the following result:

THEOREM. *The function* $\zeta_K(s)$ *is a rational function of* $T=q^{-s}$. *More precisely, there is a polynomial* P *of degree* $2g$, *where* g *is the genus of* K, *with* $P(0)=1$, *such that*

$$\zeta_K(s) = \frac{P(T)}{(1-T)(1-qT)} .$$

Furthermore, $P(1)=h$, *the order of the divisor class group* $\mathrm{Pic}^0(K)$. (See Section 7.5.)

REMARK. A celebrated theorem of A. Weil asserts in addition that $P(T)$ lies in $\mathbf{Z}[t]$ and admits a factorization over $\mathbf{C}$ of the form

$$\prod_{j=1}^{2g}(1-\alpha_j T)$$

with each α_j an algebraic integer of absolute value $q^{1/2}$. Consequently, every zero of $\zeta_K(s)$ lies on the line $\{\mathrm{Re}(s)=1/2\}$—in other words, the *Riemann hypothesis* holds for K! But a proof of this result lies far beyond the scope of this book.

(a) Show that there exist infinitely many places v of K such that $N(v)=q$. Here the norm of v simply measures the cardinality of the residue field associated with the corresponding local field K_v. [*Hint*: Suppose not. Then

$$\zeta_K(s)=\prod_{v\in S}(1-q^{-s})\cdot\prod_{v\notin S}(1-q^{-f_v s})^{-1}$$

for a finite set S, with $f_v\geq 2$ for all v outside S. Deduce from this that in fact, $\log\zeta_K(s)$ has a finite limit as $s\to 1^+$, and thus derive a contradiction to Theorem 7-19.]

(b) Show that $\zeta_K(s)$ is a meromorphic function of q^{-s}. [*Hint*: Show that the image of $|\cdot|_{\mathbf{A}_K}:\mathbf{I}_K\to\mathbf{R}_+^\times$ is $q^{\mathbf{Z}}$, and then use that $\zeta_K(s)=L(|\cdot|_{\mathbf{A}_K}^s)$.]

(c) Using part (b) and Theorem 7-19, show that $\zeta_K(s)$ takes the form given in the theorem above, with $P(q^{-s})$ an entire function.

(d) Using the functional equation for $\zeta_K(s)$, deduce the following functional equation for the numerator:

$$P(T)=q^g T^{2g}P(\frac{1}{qT}).$$

Deduce that P must be a polynomial, and (by using Theorem 7-22) that $P(1)=h$.

(e) Let χ be any idele class character of K. Show that $L(\chi)$ is a rational function of $T=q^{-s}$. [*Hint*: Reduce to the unitary case and argue as above. Provided that $\chi\neq|\cdot|_{\mathbf{A}_K}^s$, the function $L(\chi)$ is in fact a polynomial in T.]

23. Let K be a number field. For $x>0$, put

$$\pi_K(x)=\mathrm{Card}(\{P \text{ prime in } \mathfrak{o}_K : N(P)\leq x\}).$$

The "prime number theorem" for K then asserts that as $x\to\infty$,

$$\pi_K(x) \sim \frac{x}{\log x} . \tag{7.21}$$

For $K=\mathbf{Q}$, this was conjectured by Riemann and proven independently by Hadamard and de la Vallée-Poussin in 1896. The object of this exercise is to deduce this theorem from the following theorem for Dirichlet series:

THEOREM. (Tauberian Theorem for Dirichlet Series) *Let*

$$D(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$$

be a Dirichlet series with nonnegative coefficients a_n *that satisfies the following conditions:*

(i) $D(s)$ *is normally convergent in* $\{\mathrm{Re}(s) > 1\}$.

(ii) $D(s)$ *is invertible on the line* $\{\mathrm{Re}(s)=1\}$ *except for a simple pole at the point* $s=1$ *of residue* α.

Then

$$\sum_{n\leq x} a_n \sim \alpha x$$

asymptotically in x.

(a) Show that

$$\zeta_K'(s)/\zeta_K(s) = D(s) + \varphi(s)$$

for some function $\varphi(s)$ holomorphic and nonzero in $\{\mathrm{Re}(s)\geq 1\}$ and $D(s)$ the Dirichlet series defined by $a_n=\log n$, if n is the norm of some prime P, and $a_n=0$, otherwise.

(b) Using the results of Section 7.7, show that the function $D(s)$ of the previous part satisfies the hypotheses of the Tauberian theorem and has residue 1 at $s=1$. Deduce that

$$g(x) = \sum_{N(P)\leq x} \log N(P) \sim x .$$

(c) Put $b_n=a_n/\log n$. Show that for any $m\geq 1$, we have

$$\pi_K(m) = \sum_{n \le m} \frac{a_n}{\log n} = \frac{g(m)}{\log m} + h(m)$$

where

$$h(m) = \sum_{n<m} g(n)\left[\frac{1}{\log n} - \frac{1}{\log(n+1)}\right] .$$

[*Hint*: $a_n = g(n) - g(n-1)$.]

(d) Using that $g(n) \sim n$, prove Eq. 7.21 by showing that $h(m)$ is $o(m/\log m)$; that is,

$$\lim_{m \to \infty} \frac{\log m}{m} h(m) = 0 .$$

[*Hint*: Show first that

$$\left(\frac{1}{\log n} - \frac{1}{\log(n+1)}\right) \le \frac{1}{n \log^2 n}$$

for all $n > 1$.]

Appendices

The two appendices address, respectively, the elementary theory of normed linear spaces and the factorization properties of Dedekind domains. In both areas, our goal is to review fundamental definitions and results that have been used frequently in the main exposition; hence the discussions below are sharply limited. We shall indicate comprehensive sources in the references.

Appendix A: Normed Linear Spaces

In the main, this appendix addresses common topological constructs on normed linear spaces and particular aspects of L^p-spaces and L^p-duality. We show first that the topological possibilities for a finite-dimensional normed linear space X are essentially limited to one, and then discuss for general X the weak topology and the weak-star topology on the continuous dual X^*. The discussion culminates in Alaoglu's theorem. The final section defines the L^p-spaces for locally compact Hausdorff spaces and states without proof the duality theorem for spaces belonging to conjugate exponents.

A.1 Finite-Dimensional Normed Linear Spaces

If X is any normed linear space (real or complex), we let $S^1(X)$ denote the set of elements of X of norm 1. Similarly, $B^1(X)$ denotes the set of all elements of norm less than or equal to 1, the so-called *unit ball.*

Recall that $l_1(\mathbf{C}^n)$ is the complex normed linear space whose underlying vector space is $\mathbf{C}^n$ with norm given by

$$\|(a_j)\| = |a_1| + \cdots + |a_n|$$

for $(a_j)\in\mathbf{C}^n$. [We shall also write $\boldsymbol{a}$ for (a_j) when convenient.] The point of this brief discussion is to show that every complex normed linear space of dimension n is isomorphic to $l_1(\mathbf{C}^n)$ in the category of complex normed linear spaces with morphisms given as continuous linear maps. It follows from this that any two finite-dimensional complex normed linear spaces of the same dimension

are likewise isomorphic. Note that this discussion applies equally well to the category of real normed linear spaces.

We begin with some easy preliminaries. Let X be a complex normed linear space of dimension $n \geq 1$. Choose a basis $x_1, \ldots, x_n$ for X, via which we may define the following map, which at the least is an isomorphism of vector spaces:

$$\begin{aligned} \varphi : l_1(\mathbf{C}^n) &\to X \\ (a_j) &\mapsto \sum_j a_j x_j \ . \end{aligned}$$

Evidently,

$$\|\varphi((a_j))\| \leq \sup\|x_j\| \cdot \sum_j |a_j|$$

whence φ is bounded with respect to the l_1-norm and hence continuous. We wish to show more, namely that φ is an isomorphism of normed linear spaces. The key technical point lies in the following lemma:

A-1. LEMMA. *There exists a positive constant ε such that for all elements $(a_j) \in l_1(\mathbf{C}^n)$ of unit norm, $\|\varphi((a_j))\| \geq \varepsilon$.*

PROOF. As (a_j) ranges over the compact set $S^1(l_1(\mathbf{C}^n))$, $\|\varphi((a_j))\|$ at some point assumes a minimum value. This minimum cannot be zero, since the vector space isomorphism φ has trivial kernel, and the zero vector is manifestly not of unit norm. Hence the minimum is indeed a positive number ε, as claimed. ❑

We deduce from the lemma that φ is moreover a topological isomorphism as follows. Let $x \in B^1(X)$ be nonzero and suppose that $\varphi^{-1}(x) = a$. Then

$$\|\ \varphi(a/\|a\|)\ \| \geq \varepsilon$$

and so by construction,

$$\|\ \varphi^{-1}(x)\ \| = \|a\| \leq \|x\| \cdot \frac{1}{\varepsilon} \ .$$

Hence φ^{-1} is likewise bounded, and therefore continuous. Thus we have proven a fundamental result:

A-2. THEOREM. *Let X be a finite-dimensional complex normed linear space of dimension n. Then X is isomorphic to $l_1(\mathbf{C}^n)$. Consequently, any two finite-dimensional normed linear spaces of the same dimension over $\mathbf{C}$ are isomorphic.* ❑

As a further consequence of the isomorphism φ we may observe that every finite-dimensional complex normed linear space is moreover complete, and therefore a complex Banach space.

A.2 The Weak Topology

Let X be a (real or complex) normed linear space. Then the given norm defines a topology on X via the associated metric. This is called the *norm*, or *strong*, topology, and with respect to it, X is of course a locally convex topological vector space. We shall now introduce a second natural topology on X, comparable to the norm topology, but still of a somewhat different character.

DEFINITION. Let X^* be the continuous dual of X. The *weak topology* on X is defined to be the coarsest topology such that each map $x^* \in X^*$ is continuous.

Since the inverse image of any open neighborhood of 0 must be weakly open for each x^*, the weak topology has a neighborhood base at 0 given by sets of the form

$$N(0; x_1^*, \ldots, x_n^*; \varepsilon) = \{x \in X : |x_j^*(x)| < \varepsilon, j = 1, \ldots, n\}. \tag{A.1}$$

We may deduce from this that the weak topology is Hausdorff and satisfies the first axiom of countability; hence with regard to convergence we may deal with sequences rather than nets. Thus it follows at once from the definition that a sequence $\{x_j\}$ in X converges weakly (i.e., converges in the weak topology) to a point x_0 in X if and only if for each $x^* \in X^*$, we have

$$x^*(x_0) = \lim_{j \to \infty} x^*(x_j). \tag{A.2}$$

These observations yield the following fundamental result:

A-3. PROPOSITION. *Let X be as above. Then the following assertions hold:*

(i) *The weak topology is indeed weaker than the norm topology.*

(ii) *X is also a locally convex topological vector space with respect to the weak topology.*

PROOF. (i) Recall that in an arbitrary first countable topological space, the closure of a subset Y is exactly the set of points that can be obtained as the limits of convergent sequences in Y. Clearly, Eq. 2 implies that strong convergence implies weak convergence (since each x^* is continuous), and so if a subset of X is

weakly closed, it is also norm closed. Hence the weak topology is indeed weaker than the norm topology.

(ii) Let $\{(x_j,y_j)\}$ be a weakly convergent sequence in $X\times X$ with limit (x_0,y_0). Then the sequences $\{x_j\}$ and $\{y_j\}$ converge weakly to x_0 and y_0, respectively. Now since each x^* is additive, the definition of weak continuity and the ordinary continuity of addition on X with respect to the norm topology yield the weak limit

$$\{x_j+y_j\} \to x_0 + y_0 \ .$$

Hence we have the following commutative square of mappings and weak limits:

$$\begin{array}{ccc} (x_j,y_j) & \mapsto & x_j+y_j \\ \downarrow & & \downarrow \\ (x_0,y_0) & \mapsto & x_0+y_0 \end{array}$$

showing that addition is weakly continuous on $X\times X$. A similar argument shows that scalar multiplication is likewise weakly continuous, and hence X is at least a topological group with respect to the weak topology.

It remains to show that X is weakly locally convex. For this, we consider Eq. A.1. Suppose that

$$x, y \in N(0; x_1^*, \ldots, x_n^*; \varepsilon) \ .$$

Then for all indices j and real numbers t, $0\le t\le 1$, the triangle inequality yields

$$|x_j^*(tx+(1-t)y)| \le t|x_j^*(x)|+(1-t)|x_j^*(y)| \le \varepsilon$$

whence $tx+(1-t)y \in N(0;x_1^*,\ldots,x_n^*;\varepsilon)$. Hence X is locally convex. □

The weak topology on a normed linear space X also gives rise to a *weak dual*: the space of all linear maps from X to the ground field that are continuous with respect to the weak topology on X. The notation for this construction might have proved too much of a challenge (perhaps X^*_{weak}), but fortunately, the weak dual coincides with the ordinary norm dual.

A-4. PROPOSITION. *Let X be a normed linear space. Then the weak dual of X coincides with X^*, the ordinary norm dual of X.*

PROOF. Let W be an arbitrary space with topologies τ and τ' and suppose that τ is weaker than τ'. Then for any fixed topological space Y, every map $W\to Y$ that

is τ-continuous is automatically τ'-continuous: if the inverse image of every open subset of Y is open in the τ topology, it is certainly also open in the τ' topology. In particular, since the weak topology is weaker than the norm topology, every weakly continuous linear map from X to $\mathbf{C}$ is a norm continuous linear map from X to $\mathbf{C}$. Conversely, by definition of the weak topology every norm continuous functional is also weakly continuous. ❑

We show next that in a Banach space, weakly compact sets are norm closed and norm bounded. The key to this is the uniform boundedness principle, which we now recall: *Let X be a Banach space, and let Y be a normed linear space. Suppose that $\mathscr{T}$ is a subset of* Hom(X, Y), *the space of bounded operators from X to Y, such that for every $x \in X$, the set $\{T(x) : T \in \mathscr{T}\}$ is bounded in Y. Then $\mathscr{T}$ is a bounded subset of* Hom(X, Y).

A-5. PROPOSITION. *Let K be a weakly compact subset of the Banach space X. Then K is norm closed and norm bounded.*

PROOF. Since K is weakly compact, it is weakly closed, and hence norm closed. It remains to show that K is bounded. Since each element of the dual space is weakly continuous, for each element $x^* \in X$, we know that $x^*(K)$ is a compact, hence bounded, subset of $\mathbf{C}$. But consider the natural isometric embedding of K into X^{**} defined by $k(x^*) = x^*(k)$ for each $k \in K$. (The isometry, hence injectivity, follows from the Hahn-Banach extension theorem.) Under this identification, K is a subset of Hom$(X^*, \mathbf{C})$ which is bounded at each point of its domain. Hence by the uniform boundedness principle, K is norm bounded in X^{**}, which is to say norm bounded in X. ❑

A.3 The Weak-Star Topology

Let X be a (real or complex) normed linear space, with norm continuous dual X^*. Then every element $x \in X$ gives rise to an *evaluation map* $v_x \in X^{**}$ in the usual way:

$$v_x(x^*) = x^*(x)$$

for all $x^* \in X^*$. Indeed, since X is locally convex, the Hahn-Banach separation theorem asserts in particular that the mapping $x \mapsto v_x$ is an embedding. Accordingly, we shall often simply write $x(x^*)$ for $v_x(x^*)$.

DEFINITION. The *weak-star topology* on X^* is the coarsest topology such that each evaluation map v_x for $x \in X$ is continuous.

Note that in the special case that $X=X^{**}$, the weak-star and weak topologies on X^* coincide by definition. Thus they can differ only to the extent that the evaluation maps from X do not exhaust X^{**}.

We can also characterize the weak-star topology on X by limits and neighborhoods. A net $\{x_\lambda^*\}$ in X^* converges in the weak-star topology to a point x_0^* in X^* if and only if for each $x \in X$ we have

$$x_0^*(x) = \lim x_\lambda^*(x) \quad . \tag{A.3}$$

Moreover, since the inverse image under an evaluation map v_x of a neighborhood of zero in **C** must be weak-star open for each $x \in X$, the weak-star topology has a neighborhood base at 0 given by sets of the form

$$N^*(0; x_1, \ldots, x_n; \varepsilon) = \{x^* \in X: |x^*(x_j)| < \varepsilon, j = 1, \ldots, n\} . \tag{A.4}$$

Thus as above, we have that the weak-star topology is both Hausdorff and first countable. These facts suffice to prove the following result:

A-6. PROPOSITION. *Let X be as above. Then the following assertions hold:*

(i) *The weak-star topology of X^* is weaker than the weak topology.*

(ii) *X^* is a locally convex topological vector space with respect to the weak-star topology.*

PROOF. (i) Rewriting Eq. 4 explicitly in terms of evaluation maps, we have

$$N^*(0; x_1, \ldots, x_n; \varepsilon) = \{x^* \in X: |v_{x_j}(x^*)| < \varepsilon, j = 1, \ldots, n\} \ .$$

Thus we see that weak-star neighborhoods are in fact weak neighborhoods, and this proves (i).

(ii) The argument that X^* is a locally convex topological vector space with respect to the weak-star topology is entirely similar to the corresponding argument for the weak topology. ❑

We shall next show that the weak-star dual of X^* is precisely X. Note that this argument is not as shallow a formality as the proof that the weak and norm duals of X are identical. In fact, the key is the following purely linear algebraic result:

A-7. LEMMA. *Let V be a vector space over the field k, and let $f, g_1, \ldots, g_n$ be elements of the dual space. Suppose further that* $\mathrm{Ker}(f) \supseteq (\cap \mathrm{Ker}(g_j))$. *Then f lies in the span of $g_1, \ldots, g_n$.*

PROOF. By induction on n. If $n=1$, we have $\mathrm{Ker}(f)\supseteq\mathrm{Ker}(g_1)$, so that both f and g_1 factor through the induced maps $\bar{f},\bar{g}_1: V/\mathrm{Ker}(g_1)\to k$. Since the quotient space has dimension no greater then one, $\bar{f}$ is certainly a scalar multiple of $\bar{g}_1$, and hence f is likewise a scalar multiple of g_1.

Now assume that $n>1$. Let

$$f|, g_1|, \ldots, g_{n-1}|$$

denote the respective restrictions of the indicated maps to $\mathrm{Ker}(g_n)$. Then clearly,

$$\mathrm{Ker}(f|)\supseteq\bigcap_{j=1}^{n-1}\mathrm{Ker}(g_j|)$$

whence by induction, $f|$ is a linear combination of the maps $g_1|,\ldots,g_{n-1}|$. Thus for some family of scalars $\lambda_1,\ldots,\lambda_{n-1}\in k$, the map

$$\tilde{f}=f-\sum_{j=1}^{n-1}\lambda_j g_j$$

vanishes on $\mathrm{Ker}(g_n)$. But then $\mathrm{Ker}(\tilde{f})\supseteq\mathrm{Ker}(g_n)$, and so by the case $n=1$ it follows that $\tilde{f}$ is a scalar multiple of g_n. Hence f is indeed a linear combination of the g_j, as claimed. ❑

A-8. PROPOSITION. *Let X be a normed linear space. Then the weak-star dual of X^* coincides with X itself.*

PROOF. Let $x\in X$; as above, we may regard x as an element of the dual of X^* via the evaluation map. Then by definition of the weak-star topology, x is a weak-star continuous map on X^*, and so only the converse is interesting.

Let f be a weak-star continuous linear map from X^* into $\mathbf{C}$. Then

$$U=\{x^*\in X^*: |f(x^*)|<1\}$$

is weak-star open in X^* and hence contains an open neighborhood of zero of the form $N^*(0;x_1,\ldots,x_n;\varepsilon)$. Now suppose that for some $x^*\in X^*$ we have

$$x^*(x_j)=0\quad(j=1,\ldots,n)$$

which is to say that x^* lies in the kernel of each of the evaluation maps corresponding to the x_j and in particular, $x^*\in N^*(0;x_1,\ldots,x_n;\varepsilon)\subseteq U$. Then also for all scalars λ we have

$$(\lambda x^*)(x_j) = 0 \ (j = 1,\ldots,n)$$

whence $|f(\lambda x^*)|<1$ for all λ. But then in fact, $f(x^*)=0$. The upshot is that $\mathrm{Ker}(f)\supseteq(\cap\mathrm{Ker}(x_j))$, whence by the previous lemma f is a linear combination of the x_j and therefore itself a member of X, as required. ❑

The most fundamental property of the weak-star topology on the dual of a normed linear space is the following criterion for compactness:

A-9. THEOREM. (Alaoglu) *Let X be a normed linear space and let B_{X^*} denote the unit ball of the (norm) continuous dual X^*. Then*

(i) *B_{X^*} is a weak-star compact subset of X^*;*

(ii) *Any bounded and weak-star closed subset of X^* is weak-star compact.*

PROOF. (i) Let $x^*\in B_{X^*}$. Then for every $x\in B_X$, the unit ball in X, we have that $|x^*(x)|\leq 1$. Thus we obtain an injective mapping

$$B_{X^*} \to \prod_{B_X} D$$
$$x^* \mapsto x^*|_{B_X}$$

from B_{X^*} into a product of unit disks D in the complex plane. Moreover, since the weak-star topology on X^* and the product topology on the codomain are both the topology of pointwise convergence, the map above is in fact a topological isomorphism onto its image, and accordingly we may regard it as an identification. Therefore, since by Tychonoff's theorem the full domain is compact, it suffices to show that B_{X^*} is, under the given identification, a closed subset thereof.

Suppose that $\{x_j^*\}$ is a sequence in B_{X^*} convergent to some function $f:B_X\to D$. Then by pointwise convergence and the linearity of the dual elements it follows at once that

$$f(ax+by) = af(x) + bf(y)$$

whenever x, y, and $ax+by$ lie in B_X. From this it is clear that f extends uniquely by linearity from any basis contained in B_X to some element of X^*, or, to put it the other way around, f is the restriction of some unique element in X^*, which we also denote f. Moreover, since f is the weak-star limit of functionals of norm less than or equal to 1, f likewise has norm less than or equal to 1, and so is itself a member of B_{X^*}. Accordingly, B_{X^*} contains its limit points and is therefore closed, as required.

(ii) Any bounded and weak-star closed subset Y of X^* is contained in some expansion of the unit ball B_{X^*} by a positive factor λ. Since multiplication by such a scalar is a homeomorphism of X^* onto itself, Y is then a weak-star closed subset of the weak-star compact space λB_{X^*}, and hence itself weak-star compact. ❑

A.4 A Review of L^p-Spaces and Duality

Let X be a locally compact Hausdorff space. Recall that a *Radon measure* on X is a Borel measure μ that is finite on compact sets, outer regular on all Borel sets, and inner regular on all open sets. (See Section 1.2.) An integral defined with respect to a Radon measure is called a *Radon integral*. Not surprisingly, one can also develop Radon integrals as an extension of a linear functional I on $\mathscr{C}_c(X)$, the space of continuous functions on X with compact support, with the additional proviso that $I(f)\geq 0$ whenever $f\geq 0$.

Let f and g be measurable functions on X. Then we say that f and g agree *almost everywhere* (with respect to μ!) if the subset of X on which f and g disagree has measure 0. Clearly, agreement almost everywhere is an equivalence relation on the space of measurable functions on X. The quotient space modulo this relation is denoted $L(X)$. By customary abuse of language we shall often speak of elements of $L(X)$ as ordinary functions. Moreover, we admit functions $f: X\to \mathbf{R}\cup\{\pm\infty\}$ into $L(X)$, provided that the subset $Y=f^{-1}(\{\pm\infty\})$ has measure zero and that f is measurable on the complement of Y in the ordinary sense.

Let $L^1(X)\subseteq L(X)$ denote the vector space (real or complex, according to context) of integrable functions on X (with finite integral). By definition of abstract integration, $f\in L^1(X)$ if and only if $|f|\in L^1(X)$. More generally, for any real number $p\geq 1$ define $L^p(X)\subseteq L(X)$ as follows:

$$L^p(X) = \{f\in L(X): |f|^p\in L^1(X)\} .$$

One defines a norm $\| \ \|_p$ on $L^p(X)$ by the formula

$$\|f\|_p = \left\{ \int_X |f|^p \, dx \right\}^{1/p} .$$

By virtue of Minkowski's inequality, $\| \ \|_p$ is indeed a norm on $L^p(X)$, and in fact, $L^p(X)$ constitutes a Banach space with respect to this norm.

One extends these considerations to the case $p=\infty$ as follows. Assume that $f: X\to[0,\infty]$ is a measurable function. Consider the subset S of $\mathbf{R}$ defined by

$$S = \{a\in\mathbf{R}: \mu(f^{-1}(a,\infty]) = 0\} .$$

Now define s, the *essential supremum* of f, by the formula

$$s = \begin{cases} \inf S & \text{if } S \neq \varnothing \\ \infty & \text{otherwise.} \end{cases}$$

Note that if S is nonempty, then indeed $s \in S$ by virtue of the formula

$$f^{-1}([s,\infty]) = \bigcup_n f^{-1}((s+\frac{1}{n},\infty])$$

and the fact that a countable union of measurable sets is measurable. Given any $f \in L(X)$, define $\|f\|_\infty$ to be the essential supremum of $|f|$. Accordingly, set

$$L^\infty(X) = \{f \in L(X) : \|f\|_\infty \text{ is finite}\} .$$

Elements of $L^\infty(X)$ are called *essentially bounded functions*. The general inclusion

$$(f+g)^{-1}((a+b,\infty]) \subseteq f^{-1}((a,\infty]) \cup g^{-1}((b,\infty])$$

shows at once that $\| \ \|_\infty$ is indeed a norm on $L^\infty(X)$. In fact, $L^\infty(X)$ is a Banach space with respect to this norm.

Duality

We conclude this synoptic review with a key duality statement for L^p-spaces, but first we must introduce a technical restriction on our locally compact Hausdorff space X.

DEFINITION. A topological space X is called *σ-compact* if X is the countable union of compact subsets.

Clearly the metric spaces $\mathbf{R}^n$ and $\mathbf{C}^n$ are σ-compact, since each is the union of balls of integral radius. Moreover, one can show that every locally compact, σ-compact Hausdorff space is normal. We now state the main result:

A-10. THEOREM. *Let X be a locally compact, σ-compact Hausdorff space with Radon measure μ. Let p and q satisfy the relation*

$$\frac{1}{p} + \frac{1}{q} = 1$$

where $1 \le p, q \le \infty$ and $1/\infty$ is defined to be zero. Then for each pair of functions $f \in L^p(X)$ and $g \in L^q(X)$,

$$\langle f|g\rangle = \int_X f\bar{g}\,d\mu$$

is finite. Moreover, the mapping

$$\begin{aligned} L^p(X) &\to L^q(X)^* \\ f &\mapsto \langle f|-\rangle \end{aligned}$$

defines an isometric isomorphism from $L^p(X)$ to $(L^q(X))^*$.

Note that this theorem clearly extends to the case that X is the disjoint union of σ-compact sets, a condition met by every locally compact topological group G, as demonstrated by the following argument:

Let K be a compact neighborhood of the identity of G. Then K admits a symmetric subset V, also a neighborhood of the identity, which we may assume is closed and hence compact. The subset V in turn generates a subgroup H of G, which is manifestly the countable union of compact sets:

$$H = \bigcup_{j=1}^{\infty}\left(\prod_{k=1}^{j} V\right) .$$

Finally, G is the disjoint union of cosets of H, thus proving our claim.

Appendix B: Dedekind Domains

We now survey the elementary theory of Dedekind domains. In particular, we demonstrate the crucial property that the group of fractional ideals of a Dedekind domain is free on its prime ideals, and we examine the behavior of primes under extension. Throughout, all of our rings are commutative with unity.

B.1 Basic Properties

Let A be an integral domain, which is to say that $\{0\}$ is a prime ideal of A. Then a nonempty subset $S \subseteq A^*$ is called *multiplicative* if it is closed under multiplication. In this case, we can construct the ring

$$A_S = \{a/s : a \in A,\ s \in S\}$$

via the usual quotient construction: $a/s = a'/s'$ if and only if $as' = a's$. This is called the *localization of A at S*. Given any $s \in S$, we clearly have an embedding of A in A_S defined by sending $a \in A$ to $as/s \in A_S$, and one sees that we may assume that $1 \in S$.

In the particular case that $S = A^*$, the localization A_S is the full fraction field of A. This example has an important generalization. Let P be any prime ideal of A. Then $S = A - P$ is a multiplicative set. (We accept the convention that a prime ideal is a proper ideal.) In this case, we write A_P for A_S and speak of the localization of A at P.

Localization at an arbitrary multiplicative set S has the following key property with respect to prime ideals.

B-1 PROPOSITION. *Let A be an integral domain and let S be a multiplicative subset of A. Then the maps*

$$Q' \mapsto Q = Q' \cap A$$
$$Q \mapsto Q' = QA_S$$

constitute a mutually inverse pair of order-preserving bijections from the set of prime ideals of A_S to the set of prime ideals of A that have empty intersection with S.

PROOF. Exercise. ❑

A ring having exactly one maximal ideal is called a *local ring*. We see at once that in such a ring, the complement of this unique maximal ideal consists precisely of the group of units. It follows from the proposition that if P is a

prime ideal of A, then A_P has only one maximal ideal, namely PA_P. Therefore the localization of a ring at a prime ideal is always local, and if Q is any ideal of A not contained in the prime P, then clearly QA_P blows up to A_P. Thus localization at a prime ideal vastly simplifies the multiplicative structure of a ring.

REMARK. Some algebraists prefer to reserve the term *local ring* for a Noetherian ring with a unique maximal ideal; they then call what we have defined above a *quasi-local ring*.

The ideals of an integral domain and the full ring itself are determined by localization at maximal ideals in the following sense.

B-2 PROPOSITION. *Let A be an integral domain. Then*

(i) *We have that*

$$A = \bigcap_M A_M$$

where the intersection is taken over all maximal ideals of A.

(ii) *Let $J_0 \subseteq J_1$ be a chain of ideals in A such that $J_0 A_M = J_1 A_M$ for all maximal ideals M of A. Then $J_0 = J_1$.*

PROOF. Let $x = y/z$ ($y, z \in A$) lie in the given intersection, and assume that $x \in A_M$ for every maximal ideal M. Consider the set $I = \{a \in A : ay \in Az\}$, which is clearly an ideal of A. If M is any maximal ideal, then $y/z = y'/z'$ for some ring elements y' and z' with z' *not* in M. Hence $z' \in I$, and thus I does not lie in any maximal ideal. Accordingly, $I = A$, and so $1 \in I$, whence $y \in Az$ and $x = y/z \in A$. This proves part (i). The proof of part (ii) is similar, but in this case we show that for every $x \in J_1$, the ideal $I = \{a \in A : ax \in J_0\}$ is all of A, showing at once that $x \in J_0$. ❑

Local rings admit a special case that will be of utmost importance to us. A principal ideal domain having exactly one nonzero prime (hence maximal) ideal is called a *discrete valuation ring*. Note that this definition excludes fields. If the unique prime ideal of A is generated by the irreducible element π, then π is called a *uniformizing parameter* for A, and it is unique up to a factor in $A^\times$. One sees at once that every nonzero element of A factors as $u\pi^n$ for some unit u and unique nonnegative integer n; moreover, every ideal of A has the form $A\pi^n$, again for a unique n. This brings us to the key definition of this appendix.

DEFINITION. Let A be a Noetherian integral domain. Then A is called a *Dedekind domain* if for every nonzero prime ideal P of A, the localization A_P is a discrete valuation ring.

Our most interesting examples will arise shortly in connection with integral elements. For the present, we make the following elementary observations, all of which follow immediately from the first proposition above:

(i) Any principal ideal domain is a Dedekind domain.

(ii) Every prime ideal of a Dedekind domain is maximal.

(iii) The localization of a Dedekind domain at any multiplicative set is likewise a Dedekind domain.

Our goal for this section is to demonstrate some fundamental equivalent characterizations of a Dedekind domain, but before doing so, we must review the notion of an integral element over a ring.

Integral Elements

Let B be an extension of the ring A, so that inclusion is a unital ring homomorphism. Then an element $x \in B$ is said to be *integral over* A if there exists a monic polynomial $p(t) \in A[t]$ such that $p(x)=0$.

B-3 PROPOSITION. *Let A, B, and x be as above. Then the following four statements are equivalent:*

(i) *The element x is integral over A.*

(ii) *The ring $A[x] \subseteq B$ is finitely generated as a module over A.*

(iii) *The ring $A[x]$ is contained in a subring A' of B that is finitely generated as a module over A.*

(iv) *There exists an $A[x]$-module L, finitely generated over A, such that the only element of A that annihilates L is zero.*

PROOF. That (i) implies (ii) follows at once from the observation that if x satisfies a monic polynomial of degree n in $A[t]$, then by Euclidean division $A[x]$ is generated by $1, x, \ldots, x^n$ as a module over A. Clearly, (ii) implies (iii), and (iii) implies (iv). (For the latter, take $L=A[x]$ itself, which contains 1.) Thus it remains only to show that (iv) implies (i).

Let L be as stated, and let $b_1, \ldots, b_r$ be a set of generators for L over A. Then for each index i we have an equation

$$xb_i = \sum_{j=1}^{r} \lambda_{ij} b_j$$

for some $\lambda_{ij} \in A$. Now consider the $r \times r$ matrix M defined by

$$M = (x\delta_{ij} - \lambda_{ij})$$

where δ_{ij} is the Kronecker delta. Then we have the matrix equation

$$M\boldsymbol{b} = \boldsymbol{0}$$

where $\boldsymbol{b}$ is the column vector whose components are $b_1, \ldots, b_r$. Multiplying both sides of this equation by the adjoint of M shows that $d = \det(M)$ annihilates every b_i and hence all of L. By hypothesis we then must have that $d = 0$, and therefore x satisfies the monic polynomial $\det(t\delta_{ij} - \lambda_{ij})$ in $A[t]$. Thus x is integral over A, and this completes the proof. ❑

If $x,y \in B$ are both integral over A, then $A[x,y]$ is finitely generated as an A-module, and hence by part (iii) above, their sum, difference, and product are likewise integral over A. Thus we have the following immediate corollary:

B-4 COROLLARY. *Let A and B be as above. Then the set of all elements of B that are integral over A is a subring of B containing A.* ❑

The ring consisting of all elements of B integral over A is called the *integral closure* of A in B. One deduces easily from the proposition above that the operation of taking the integral closure within a fixed extension is idempotent. If A is equal to its integral closure in an extension B, we say that A is *integrally closed in B*. We say that an integral domain is *integrally closed* (without reference to an extension) if it is integrally closed in its fraction field. We leave it to the reader to show that every unique factorization domain is integrally closed.

Characterization of Dedekind Domains

With the notion of integral closure in hand, we can now state our main result on the characterization of Dedekind domains.

B-5 THEOREM. *Let A be an integral domain, and assume that A is not a field. Then the following three statements are equivalent:*

(i) *A is a Dedekind domain.*

(ii) *For each maximal ideal M of A, the localization A_M is a discrete valuation ring, and each nonzero element of A is contained in only finitely many prime ideals.*

(iii) *A is Noetherian, integrally closed, and every nonzero prime ideal is maximal.*

Before proving this, we need to do a little more elementary commutative algebra.

B-6 PROPOSITION. *Let A be a Noetherian ring. Then*

(i) *Every ideal of A contains a product of prime ideals.*

(ii) *There exist distinct prime ideals $P_1, \dots, P_r$ and corresponding positive integers $m_1, \dots, m_r$ such that*

$$\{0\} = \prod_{j=1}^{r} P_j^{m_j} .$$

Assume further that A has zero divisors and that every nonzero prime ideal of A is maximal. Let the prime ideals $P_1, \dots, P_r$ and integers $m_1, \dots, m_r$ be as above. Then we have, moreover, that

(iii) $A \cong \prod_{j=1}^{r} A/P_j^{m_j}$.

(iv) *The prime ideals $P_1, \dots, P_r$ are the only prime ideals of A.*

PROOF. Part (i) follows by Noetherian induction: If I is maximal among ideals not containing a product of primes, then there exist x and y in A such that neither x nor y lies in I, but the product xy does. Then $(Ax+I)(Ay+I) \subseteq I$, and both factors, by virtue of being strictly larger than I, contain products of primes; hence so does I—a contradiction. Part (ii) is an immediate corollary. Part (iii) then holds in consequence of the Chinese remainder theorem, once we note that if I and J are distinct maximal ideals of A, then I^m and J^n remain comaximal for all positive m and n. Finally, part (iv) follows at once from part (iii). ❑

B-7 COROLLARY. *Let A be a Noetherian ring for which every nonzero prime ideal is maximal. Then every nonzero ideal of A is contained in only finitely many prime ideals. In particular, every nonzero element of A is contained in only finitely many prime ideals.*

PROOF. Let I be a nonzero ideal of A. If I is prime, it is contained in only one proper ideal, namely I itself. Otherwise, A/I is not an integral domain, and we can apply parts (ii) through (iv) of the preceding proposition to this quotient. ❑

We may now proceed to the proof of the main theorem.

PROOF OF THEOREM. (i)$\Rightarrow$(ii). If A is a Dedekind domain, it certainly satisfies the condition of the preceding corollary, and hence assertion (ii) clearly holds

for A. (Note that $\{0\}$ is *not* a maximal ideal, whence the localization statement.)

(ii)$\Rightarrow$(iii). First, since A is the intersection of its localizations at maximal ideals, each of which is integrally closed by virtue of being a unique factorization domain, we have that A itself is integrally closed. Second, if $P \subset Q$ is any proper chain consisting of a prime ideal P and maximal ideal Q, then $PA_Q \subset QA_Q$ is likewise a proper chain of prime ideals in the discrete valuation ring A_Q—an impossibility. Hence every prime ideal of A is maximal, and it only remains to show that A is Noetherian.

Let I be any nonzero ideal in A and let $x \in I$, with x itself nonzero. Then there exist only finitely many prime ideals $P_1,\ldots,P_r$ of A that contain I. At each corresponding localization—which is a principal ideal domain—we have

$$IA_{P_j} = y_j A_{P_j}$$

for some $y_1,\ldots,y_r$, each of which, as one shows easily, we may assume also to lie in I. Now consider the ideal

$$J = Ax + Ay_1 + \cdots + Ay_r$$

which is clearly contained in I. On the one hand, if P is any prime ideal of A not containing x, then JA_P and IA_P both blow up to A_P. On the other hand, if P is any prime ideal of A that does contain x, then $P=P_j$ for some j, and by construction,

$$y_j A_P \subseteq JA_P \subseteq IA_P = y_j A_P$$

and again $JA_P = IA_P$. Thus $J \subseteq I$ constitutes a chain of ideals that collapses locally at every prime ideal, and therefore $J=I$ by Proposition B-2. Accordingly, our original ideal I is finitely generated, whence A is Noetherian.

(iii)$\Rightarrow$(i). Since A is given as Noetherian, we need only show that for each nonzero prime ideal P, the localization A_P is a discrete valuation ring. We know already that A_P has a unique prime ideal, because the nonzero primes of A are maximal by hypothesis. Since this localization is also integrally closed and Noetherian, the proof of the characterization theorem is complete if we can show that any Noetherian, integrally closed domain having precisely one nonzero prime ideal is also a principal ideal domain. Let B be such a ring, with Q its unique nonzero prime.

Given $x \in B - B^\times$, consider the nontrivial quotient B/Bx as a module over B. For each nonzero element $y + Bx$ in this quotient, let $I(y) \subseteq B$ denote its annihilator. Then because B is assumed Noetherian, among these annihilators there is a maximal element, I_ω, corresponding to, say, $y_\omega + Bx \in (B/Bx)^*$. One checks readily that I_ω is prime and hence equal to Q. So $Qy_\omega \subseteq Bx$, while y_ω itself does

not lie in Bx. Thus $z=y_\omega/x$ does not lie in B, and therefore z cannot be integral over B. But certainly $Qz\subseteq B$, whence Qz is an ideal of B. We claim that in fact, $Qz=B$. Assume contrariwise that $Qz\subseteq Q$. Then we have:

- Qz is a $B[z]$-module.
- Qz is finitely generated over B.

Since B is an integral domain, the final statement of Proposition B-3 yields a contradiction: namely, that z is integral over B. Thus $Qz=B$, and setting $\pi=z^{-1}$, we have $Q=B\pi$ (and in fact, π will be our uniformizing parameter).

We now complete the proof that B is a discrete valuation ring. Let I be any nonzero ideal of B. Then $I=Iz^{-1}z\subseteq Iz$, whence we have an ascending chain of B-modules

$$I\subseteq Iz\subseteq Iz^2\subseteq\cdots$$

which must become stationary. But if $Iz^n=Iz^{n+1}$, then Iz^n is a $B[z]$-module, finitely generated over B, and again we have the contradiction that z is integral over B. Hence only a finite part of this chain can remain in B. So assume that for some nonnegative integer n,

$$Iz^n\subseteq B \quad \text{but} \quad Iz^{n+1}\not\subseteq B\,.$$

Then it cannot be the case that $Iz^n\subseteq Q=B\pi$, or else multiplying by $z=\pi^{-1}$ yields another contradiction, and therefore $Iz^n=B$. This to say that $I=B\pi^n$. Hence B is principal, and the proof is complete. ❑

Factorization of Ideals

We shall now develop another critical property of a Dedekind domain. The point is that while a Dedekind domain need not exhibit unique factorization at the level of elements, it does so nonetheless at the level of ideals.

B-8 PROPOSITION. *Let A be a Dedekind domain. Then every nonzero ideal I of A has a unique factorization into a product of prime ideals. In fact, the ideals appearing in this factorization are precisely those prime ideals containing I.*

PROOF. Clearly we may assume that I is a proper ideal. Then I is at least contained in some prime ideal, and Corollary B-7 implies that there are only finitely many such primes. Let these be $P_1,\ldots,P_r$. They are also precisely the primes of A/I, and we know from Proposition B-6 that

$$I\supseteq\prod_{j=1}^{r}P_j^{n_j}$$

for some positive integers n_j. By the Chinese remainder theorem,

$$B = A / \prod_{j=1}^{r} P_j^{n_j} \cong \prod_{j=1}^{r} A / P_j^{n_j}$$

and by localization it is easy to see that every ideal in the factor rings appearing on the right takes the form

$$P_j^{m_j} / P_j^{n_j}$$

for some nonnegative m_j. Hence the image of I in B takes the form

$$\prod_{j=1}^{r} P_j^{m_j} / P_j^{n_j}$$

and therefore

$$I = \prod_{j=1}^{r} P_j^{m_j} .$$

We see at this point that the m_j are in fact positive, or else we would contradict the hypothesis that I is contained in each of the P_j. This shows the existence of the asserted prime factorization.

We can easily deduce uniqueness, again by localization. Suppose that

$$\prod_{j=1}^{r} P_j^{m_j} = \prod_{j=1}^{s} Q_j^{m'_j}$$

for a second family of prime ideals $\{Q_j\}$. Then localizing at any P_j yields, on the left-hand side,

$$A_{P_j} \pi_j^{m_j}$$

where π_j is the uniformizing parameter for the local ring A_{P_j}. Hence each P_j must correspond to a Q_j, and corresponding factors must manifest the same exponent. This completes the proof. ❑

REMARK. A strong form of the converse of this proposition holds: an integral domain in which every ideal is the product of prime ideals is necessarily a Dedekind domain.

Fractional Ideals and the Ideal Class Group

Let A be a Dedekind domain with field of fractions K. A *fractional ideal* of K is a nonzero finitely generated A-submodule of K. Let J_K denote the set of all such fractional ideals, the so-called *ideal group* of K. This clearly contains all the ideals of A and, in particular, A itself.

Given $I,J\in J_K$, define the product IJ as for ordinary ideals; this clearly remains in J_K. Moreover, for $I\in J_K$, define $I^{-1}=\{x\in K\colon Ix\subseteq A\}$. One checks easily that $I^{-1}\in J_K$, but perhaps it is not obvious that $I^{-1}I=A$. For ordinary ideals this follows from Proposition B-8 by localization; for arbitrary elements of J_K we need an extension of the cited proposition. This is given by the first part of the following theorem.

B-9 THEOREM. *Let A and K be as above. Then every element of $I\in J_K$ has a unique factorization of the form*

$$I=\prod_{j=1}^{r}P_j^{m_j}$$

where the exponents m_j may be positive or negative. Consequently, J_K is a free abelian group on the prime ideals of A.

PROOF. We can construct an element $x\in A$ such that $Ix\subseteq A$. Noting that $I=(Ix)(Ax)^{-1}$, we may then apply Proposition B-8 to both Ix and Ax to get our factorization. The rest is a straightforward exercise. ❑

Elements of the form Ax in J_K, with $x\in K^*$ are called *principal fractional ideals*, and these constitute a subgroup denoted P_K. The quotient $Cl_K=J_K/P_K$ is the familiar *ideal class group* of K. Note well that for a general Dedekind domain, Cl_K need not be finite. This shows that one essentially needs some analysis to supplement the abstract algebra in Chapter 5.

B.2 Extensions of Dedekind Domains

In this section we give some further fundamental definitions and state, without proof, some key results that arise in connection with extensions of Dedekind domains. Indeed, the theorems that appear here in essence define our interest in this rich class of rings.

Throughout, let A be a Dedekind domain with fraction field K, and let L/K be a finite extension of K. Then the integral closure of A in L is a subring of L, which we denote B. Clearly, $A\subseteq B$. The following theorem is paramount; it has the immediate particular consequence that for a global field K, the ring of integers $\mathfrak{o}_K$ is a Dedekind domain.

B-10 THEOREM. *Let the ring extension B/A and the field extension L/K be given as above. Then B is also a Dedekind domain.*

While we omit the proof, we will remark that one approach to proving this result is to advance in two steps by introducing an intermediate field E such that one story of the resulting tower is separable, while the other is purely inseparable. In the separable case, we may use the nondegeneracy of the trace map to show that the corresponding integral closure is Noetherian, and then proceed to show that it satisfies part (iii) of our characterization of Dedekind domains (Theorem B-5). In the purely inseparable case, we may use part (ii) of our characterization: the argument is reducible by localization to the case that A is a discrete valuation ring, and one then shows that B is likewise a discrete valuation ring.

From this theorem and the results of the preceding section, we have at once that given any prime ideal P of A,

$$PB = \prod_{j=1}^{g} Q_j^{e_j}$$

where $Q_1, \ldots, Q_g$ are the prime ideals of B that lie above (that is, contain) P. Hence in this entirely algebraic setting we now become reacquainted with two old friends from Chapter 4.

DEFINITIONS. The number e_j defined above is called the *ramification index* of Q_j over A. The number

$$f_j = (B/Q_j : A/P)$$

(that is, the degree of the extension of residue fields) is called the *residual degree* of Q_j over A.

Of course, every prime Q of B lies over some prime P of A, namely $Q \cap A$. Thus Q is said to be *ramified* over A if Q has ramification index greater than one or if the corresponding extension of residue fields fails to be separable. Otherwise, we say that Q is *unramified* over A. In the same vein, a prime P of A is *ramified* in B if it is divisible by a prime of B ramified over A; otherwise, P is *unramified*.

We have these familiar-looking results that relate ramification index to residual degree:

B-11 THEOREM. *Let P and $Q_1, \ldots, Q_g$ be as above. Then the following statements hold:*

(i) *The summation* $\sum e_j f_j$ *equals the dimension of* B/PB *over the residue field* A/P *and, moreover, is bounded by the degree of* L *over* K.

(ii) *If* L/K *is separable, then in fact,* $\sum e_j f_j = (L:K)$.

(iii) *If* L/K *is Galois, then all of the* e_j *have a common value* e *and all of the* f_j *have a common value* f; *moreover,* $efg=(L:K)$.

The Norm of an Ideal

Again A is a Dedekind domain with fraction field K, L/K is a finite extension of K, and B is the integral closure of A in L. Recall that for any $x \in L$,

$$N_{L/K}(x) \quad \text{and} \quad \mathrm{tr}_{L/K}(x)$$

the norm and the trace of x, are, respectively, the determinant and the trace of the K-linear endomorphism of L that sends $y \in L$ to xy. One knows that

$$N_{L/K}(x) = \left(\prod \sigma(x)\right)^{[L:K]_i} \quad \text{and} \quad \mathrm{tr}_{L/K}(x) = [L:K]_i \sum \sigma(x)$$

where both sum and product are taken over a full set of embeddings of L over K into a fixed algebraic closure of K, and $[L:K]_i$ is the inseparable degree of the extension. It follows at once from these formulas that both maps send elements of B into A.

We may extend the norm map $N_{L/K}: L \to K$ to ideals. If I is an ideal of B, define $N_{L/K}(I)$ to be the ideal of A generated by all of the images $N_{L/K}(x)$, where x ranges over I. In the special case that $K=\mathbf{Q}$, the ideal $N_{L/K}(I)$ is contained in $\mathbf{Z}$ and therefore is generated by a unique positive integer, which we shall denote simply $N(I)$. This is called the *absolute norm* of an integral ideal in a number field.

We summarize the most important properties of the norm and absolute norm for ideals in the two following propositions.

B-12 Proposition. *Let the extensions* B/A *and* L/K *be given as above and assume further that the latter is separable. Suppose that* I *is a nonzero ideal of* B *with prime factorization*

$$I = \prod_{j=1}^{r} Q_j^{m_j} .$$

Put $P_j = Q_j \cap A$ *and set* f_j *equal to the residual degree of* Q_j *over* A. *Then*

$$N_{L/K}(I) = \prod_{j=1}^{r} P_j^{m_j f_j} .$$

B-13 PROPOSITION. *Let K be a number field and let A be the integral closure of* $\mathbf{Z}$ *in K. Then for any nonzero ideal I of A, we have* $N(I) = \text{Card}(A/I)$.

The Different and the Discriminant

The extensions A/B and L/K remain as above, with the continuing assumption that L/K is separable. If J is any subset of L, then J' denotes its *dual subset*, which is defined by

$$J' = \{x \in L : \text{tr}_{L/K}(xJ) \subseteq A\} .$$

One can show that if J is a fractional ideal of L, then J' is likewise a fractional ideal of L. The dual subset corresponding to B itself is called the *inverse different* of B/A. The *different* of the extension, denoted $\mathcal{D}_{B/A}$, is then the inverse fractional ideal of the inverse different. Since $\mathcal{D}_{B/A}$ is the inverse of a fractional ideal that contains 1, it is in fact an ideal of B, and one can show that this ideal is determined locally.

The following general relation shows how the different is fundamental to the calculation of the dual of *any* fractional ideal J of L:

$$J' = (\mathcal{D}_{B/A})^{-1} J^{-1} .$$

Moreover, one has this essential connection with ramification:

B-14 THEOREM. *Let Q be a prime ideal of B. Then Q is ramified if and only if Q divides the different* $\mathcal{D}_{B/A}$. *In fact,* Q^{e-1} *divides* $\mathcal{D}_{B/A}$, *where e is the ramification index of Q over A.*

REMARK. As an immediate corollary, we have that only finitely many primes of B are ramified over A.

We now develop one further ring invariant. Let $x_1, \ldots, x_n$ be a basis for L over K. Then

$$\Delta(x_1, \ldots, x_n) = \det(\text{tr}_{L/K}(x_i x_j))_{1 \le i,j \le n}$$

lies in K and is called the *discriminant* of the basis $x_1, \ldots, x_n$. If each x_i lies in B, then $\Delta(x_1, \ldots, x_n)$ lies in A. Thus as $x_1, \ldots, x_n$ range over all bases of L over K that are contained in B, the elements $\Delta(x_1, \ldots, x_n)$ generate an ideal of A, denoted $\Delta(B/A)$ and called the *discriminant ideal.* This again may be determined locally, and the discriminant gives us a criterion for ramification at the lower level:

B-15 THEOREM. *Let P be a prime ideal of A. Then P ramifies in B if and only if P contains the discriminant ideal* $\Delta(B/A)$.

Finally, we state the relation between the different and the discriminant; this is mediated by the norm:

B-16 THEOREM. *Let the rings A and B and the separable extension L/K be as above. Then we have that*

$$N_{L/K}(\mathcal{D}_{B/A}) = \Delta(B/A) .$$

That is, the discriminant is the norm of the different.

The reader should refer to the exercises from Chapter 4 for a development of the different and the discriminant for the integers of local and global fields.

References

Artin, Emil. *The Gamma Function.* (Translated by Michael Butler.) New York: Holt, Rinehart and Winston, 1964.

Artin, Emil. *Algebraic Numbers and Functions.* New York: Gordon and Breach, 1967.

Aupetit, Bernard. *A Primer on Spectral Theory.* New York: Springer-Verlag, 1991.

Bruhat, F. *Lectures on Lie Groups and Representations of Locally Compact Groups.* Bombay: Tata Institute of Fundamental Research, 1968.

Cartan, H. and R. Godement. Théorie de la dualité et analyse harmonique dans les groupes abéliens localement compacts. Ann. Sci. Ecole Norm. Sup., 64(3), 79–99, 1947.

Cassels, J.W.S. and A. Fröhlich, eds. *Algebraic Number Theory.* New York: Academic Press, 1968.

Dikranjan, Dikran N., Ivan R. Prodanov, and Luchezar N. Stoyanov. *Topological Groups: Characters, Dualities, and Minimal Group Topologies.* New York: Marcel Dekker, Inc., 1990.

Folland, Gerald B. *Real Analysis: Modern Techniques and Their Applications.* New York: John Wiley and Sons, 1984.

L.J. Goldstein. *Analytic Number Theory.* New Jersey: Prentice-Hall, 1971.

Gorenstein, Daniel. *Finite Groups.* New York: Harper and Row, 1968.

Hall, M. *The Theory of Groups.* New York: MacMillan, 1959.

Hecke, E. *Mathematische Werke.* Göttingen: Vandenhoeck & Ruprecht, 1959.

Janusz, Gerald J. *Algebraic Number Fields.* New York: Academic Press 1973.

Ireland, Kenneth and Michael Rosen. *A Classical Introduction to Modern Number Theory* (Second Edition). New York: Springer-Verlag, 1990.

Kaplansky, Irving. *Commutative Rings* (Revised Edition). Chicago: The University of Chicago Press, 1974.

Koblitz, Neal. *p-adic Numbers, p-adic Analysis, and Zeta-Functions* (Second Edition). New York: Springer-Verlag, 1984.

Lang, Serge. *Algebraic Number Theory.* Massachusetts: Addison-Wesley, 1970.

Lorch, Edgar Raymond. *Spectral Theory.* New York: Oxford University Press, 1962.

Pedersen, Gert K. *Analysis Now.* New York: Springer-Verlag, 1989.

Pontryagin, L. *Topological Groups.* (Translated from the Russian by Emma Lehmer.) Princeton: Princeton University Press, 1939.

Rudin, Walter. *Real and Complex Analysis.* New York: McGraw-Hill, 1966.

Ribes, L. *Introduction to Profinite Groups and Galois Cohomology.* Kingston, Ontario: Queen's University, 1970.

Rudin, Walter. *Fourier Analysis on Groups.* New York: John Wiley & Sons, 1962; Wiley Classics Library Edition, 1990.

Serre, J.-P. *Corps locaux.* Paris: Hermann, 1968.

Serre, J.-P. *Abelian l-Adic Representations and Elliptic Curves* (Second Edition). Massachusetts: Addison-Wesley, 1989.

Serre, J.-P. *Galois Cohomology.* (Translated from the French by Patrick Ion, with new additions.) New York: Springer-Verlag, 1997.

Shatz, S. *Profinite Groups, Arithmetic and Geometry.* Princeton: Princeton University Press, 1972.

Tate, J. *Fourier Analysis in Number Fields and Hecke's Zeta Function.* Thesis, Princeton University, 1950.

Tate J. "Local Constants" in *Algebraic Number Fields*, ed. by A. Fröhlich, New York: Academic Press, 1977.

Weil, André. *L'intégration dans les groupes topologiques et ses applications.* Paris: Hermann, 1965.

Weil, André. *Basic Number Theory* (Third Edition). New York: Springer-Verlag. 1974.

Suggestions for Further Reading

To aid the reader we list below selected topics and corresponding references that are natural to pursue after this book. The list is not comprehensive, and we have certainly omitted some valuable and beautiful sources, especially where a heftier background is required.

—Topic 1: Lie Groups

These ubiquitous topological groups are characterized by being locally Euclidean. Suggested texts are:

Chevalley, C. Theory Lie Groups, I. Princeton: Princeton University Press, 1946.

Dieudonné, J. *Sur les groupes classiques*. Paris: Hermann, 1973.

Serre, J.-P. *Lie Groups and Lie Algebras* (Second Edition). New York: Springer-Verlag, 1992. (This book also develops the parallel theory of p-adic analytic groups.)

—Topic 2: Topological Transformations Groups

Koszul, J.-L. *Lectures on Groups of Transformations*. Bombay: Tata Institute of Fundamental Research, 1965.

Montgomery, D and L. Zippin. *Topological Transformation Groups*. Huntington, New York: Robert Krieger Publishing Company, 1974. (This contains a discussion of Hilbert's fifth problem.)

—Topic 3: Cohomology of Profinite Groups

Serre, J.-P. *Galois Cohomology*. (See references above.)

—Topic 4: Unitary Representations

Bruhat, F. *Lectures on Lie Groups and Representations of Locally Compact Groups*. (See references above.)

Knapp, A.W. *Representation Theory of Semisimple Groups: An Overview Bases on Examples*. Princeton: Princeton University Press, 1986.

—Topic 5: Discrete Subgroups of Lie Groups

This subject is a vast generalization of the analysis of unit groups as lattices in Euclidean spaces.

Borel, A. *Introduction aux groupes arithmétiques*. Paris: Hermann, 1969.

Raghunathan, M.S. *Discrete Subgroups of Lie Groups*. New York: Springer-Verlag, 1972.

Zimmer, R. *Ergodic Theory and Semisimple Groups*. Boston: Birkhäuser, 1984.

—Topic 6: Class Field Theory

Artin, E. and J. Tate. *Class Field Theory*. New York: W. A. Benjamin, 1968.

Lang, S. *Algebraic Number Theory*. (See references above.)

Langlands, R.P. "Abelian Algebraic Groups" in the Olga Taussky-Todd memorial volume of the Pacific Journal of Mathematics, 1998. (This work

treats the case of tori, the basic case to be understood before tackling the general philosophy of the author as it applies to the still open nonabelian case.)

Serre, J.-P. *Corps locaux.* (See references above.)

Weil, A. *Basic Number Theory.* (See references above.)

—Topic 7: Cyclotomic Fields and p-adic L-functions

Iwasawa, K. *Lectures on p-adic L-functions.* Princeton: Princeton University Press, 1972.

Lang, S. *Cyclotomic Fields I and II* (Combined Second Edition). New York: Springer-Verlag, 1990.

de Shalit, E. *Iwasawa Theory of Elliptic Curves with Complex Multiplication.* New York: Academic Press, 1987.

Washington, L. *Cyclotomic Fields.* New York: Springer-Verlag, 1982.

—Topic 8: Galois Representations and L-functions

Serre, J.-P. *Abelian l-Adic Representations and Elliptic Curves.* (See references above.)

—Topic 9: The Analytic Theory of L-functions

Apostol, T. *Modular Functions and Dirichlet Series in Number Theory* (Second Edition). New York: Springer-Verlag, 1990.

Davenport, H. *Multiplicative Number Theory.* New York: Springer-Verlag, 1980.

Murty, Mr. R. and V. K. Murty. *Nonvanishing of L-functions and Applications.* Boston: Birkhäuser, 1997.

Siegel, C.L. *On Advanced Analytic Number Theory* (Second Edition). Bombay: Tata Institute of Fundamental Research, 1990.

Titchmarsh, E.C. *The Theory of the Riemann Zeta Function* (Second Edition). Edited and with a preface by D.R. Heath-Brown. New York: Oxford University Press, 1986.

—Topic 10: $\mathrm{SL}_2(\mathbf{R})$ and Classical Automorphic Forms

Borel, A. *Automorphic Forms on* $\mathrm{SL}_2(\mathbf{R})$. Cambridge: Cambridge University Press, 1997.

Hida, H. *Elementary Theory of L-functions and Eisenstein Series.* Cambridge: Cambridge University Press, 1993.

Iwaniec, H. *Topics in Classical Automorphic Forms.* Providence: American Mathematical Society, 1997.

Lang, S. $\mathrm{SL}_2(\mathbf{R})$. (Reprinted from 1975.) New York: Springer-Verlag, 1985.

Shimura, G. *Introduction to the Arithmetic Theory of Automorphic Forms.* (Reprinted from 1971.) Princeton: Princeton University Press, 1994.

Weil, A. *Dirichlet Series and Automorphic Forms.* New York: Springer-Verlag, 1971.

—Topic 11: Automorphic Forms via Representation Theory

Bailey, T.N. and A.W. Knapp, eds. *Representation Theory and Automorphic Forms.* Providence: American Mathematical Society, 1997.

Borel, A. and W. Casselman, eds. *Automorphic Forms, Representation and L-functions I, II.* Providence: American Mathematical Society, 1979.

Bump, D. *Automorphic Forms and Representations.* Cambridge: Cambridge University Press, 1997.

Gelbart, S. *Automorphic Forms on Adele Groups.* Princeton: Princeton University Press, 1975.

Gelbart S. and F. Shahidi. *Analytic Properties of Automorphic L-functions.* Boston: Academic Press, 1988.

Godement, R. *Notes on Jacquet-Langlands Theory.* (Mimeographed notes.) Princeton: Institute of Advanced Study, 1970.

Jacquet, H. and R.P. Langlands. *Automorphic Forms on* GL(2). New York: Springer-Verlag, 1970.

Langlands, R.P. *Euler Products.* New Haven: Yale University Press, 1971.

FINAL REMARK. There are also connections of Tate's thesis with string theory. For instance, see:

Vladimirov, V.S. "Freund-Witten Adelic Formulas for Veneziano and Virasoro-Shapiro Amplitudes." Russian Mathematical Surveys, 48(6), 3–38, 1993.

Index

O

P

Q

R

Graduate Texts in Mathematics

(continued from page ii)

120 ZIEMER. Weakly Differentiable Functions: Sobolev Spaces and Functions of Bounded Variation.
121 LANG. Cyclotomic Fields I and II. Combined 2nd ed.
122 REMMERT. Theory of Complex Functions. *Readings in Mathematics*
123 EBBINGHAUS/HERMES et al. Numbers. *Readings in Mathematics*
124 DUBROVIN/FOMENKO/NOVIKOV. Modern Geometry—Methods and Applications. Part III.
125 BERENSTEIN/GAY. Complex Variables: An Introduction.
126 BOREL. Linear Algebraic Groups. 2nd ed.
127 MASSEY. A Basic Course in Algebraic Topology.
128 RAUCH. Partial Differential Equations.
129 FULTON/HARRIS. Representation Theory: A First Course. *Readings in Mathematics*
130 DODSON/POSTON. Tensor Geometry.
131 LAM. A First Course in Noncommutative Rings.
132 BEARDON. Iteration of Rational Functions.
133 HARRIS. Algebraic Geometry: A First Course.
134 ROMAN. Coding and Information Theory.
135 ROMAN. Advanced Linear Algebra.
136 ADKINS/WEINTRAUB. Algebra: An Approach via Module Theory.
137 AXLER/BOURDON/RAMEY. Harmonic Function Theory.
138 COHEN. A Course in Computational Algebraic Number Theory.
139 BREDON. Topology and Geometry.
140 AUBIN. Optima and Equilibria. An Introduction to Nonlinear Analysis.
141 BECKER/WEISPFENNING/KREDEL. Gröbner Bases. A Computational Approach to Commutative Algebra.
142 LANG. Real and Functional Analysis. 3rd ed.
143 DOOB. Measure Theory.
144 DENNIS/FARB. Noncommutative Algebra.
145 VICK. Homology Theory. An Introduction to Algebraic Topology. 2nd ed.
146 BRIDGES. Computability: A Mathematical Sketchbook.
147 ROSENBERG. Algebraic K-Theory and Its Applications.
148 ROTMAN. An Introduction to the Theory of Groups. 4th ed.
149 RATCLIFFE. Foundations of Hyperbolic Manifolds.
150 EISENBUD. Commutative Algebra with a View Toward Algebraic Geometry.
151 SILVERMAN. Advanced Topics in the Arithmetic of Elliptic Curves.
152 ZIEGLER. Lectures on Polytopes.
153 FULTON. Algebraic Topology: A First Course.
154 BROWN/PEARCY. An Introduction to Analysis.
155 KASSEL. Quantum Groups.
156 KECHRIS. Classical Descriptive Set Theory.
157 MALLIAVIN. Integration and Probability.
158 ROMAN. Field Theory.
159 CONWAY. Functions of One Complex Variable II.
160 LANG. Differential and Riemannian Manifolds.
161 BORWEIN/ERDÉLYI. Polynomials and Polynomial Inequalities.
162 ALPERIN/BELL. Groups and Representations.
163 DIXON/MORTIMER. Permutation Groups.
164 NATHANSON. Additive Number Theory: The Classical Bases.
165 NATHANSON. Additive Number Theory: Inverse Problems and the Geometry of Sumsets.
166 SHARPE. Differential Geometry: Cartan's Generalization of Klein's Erlangen Program.
167 MORANDI. Field and Galois Theory.
168 EWALD. Combinatorial Convexity and Algebraic Geometry.
169 BHATIA. Matrix Analysis.
170 BREDON. Sheaf Theory. 2nd ed.
171 PETERSEN. Riemannian Geometry.
172 REMMERT. Classical Topics in Complex Function Theory.
173 DIESTEL. Graph Theory.
174 BRIDGES. Foundations of Real and Abstract Analysis.
175 LICKORISH. An Introduction to Knot Theory.
176 LEE. Riemannian Manifolds.
177 NEWMAN. Analytic Number Theory.
178 CLARKE/LEDYAEV/STERN/WOLENSKI. Nonsmooth Analysis and Control Theory.
179 DOUGLAS. Banach Algebra Techniques in Operator Theory. 2nd ed.

- 180 SRIVASTAVA. A Course on Borel Sets.
- 181 KRESS. Numerical Analysis.
- 182 WALTER. Ordinary Differential Equations.
- 183 MEGGINSON. An Introduction to Banach Space Theory.
- 184 BOLLOBAS. Modern Graph Theory.
- 185 COX/LITTLE/O'SHEA. Using Algebraic Geometry.
- 186 RAMAKRISHNAN/VALENZA. Fourier Analysis on Number Fields.
- 187 HARRIS/MORRISON. Moduli of Curves.
- 188 GOLDBLATT. Lectures on the Hyperreals: An Introduction to Nonstandard Analysis.
- 189 LAM. Lectures on Modules and Rings.